MOBILE DEVICES POLICY

2023-24

THE HAMMOND SCHOOL LTD., MANNINGS LANE, CHESTER, CH2 4ES

Telephone: 01244 305350 | Web: www.thehammondschool.co.uk | Email: contact@thehammondschool.co.uk

This policy has been updated to comply with changes guidance as viewed in Keeping Children Safe in Education 2023 and supports the increased filtering and monitoring of online resources and access. This policy should be read in conjunction with The Hammond's Internet Filtering Policy.

Objectives

The Hammond aims to ensure secure access to ICT for all students. This policy outlines the acceptable use of internet and electronic mail facilities, file-servers, messaging services, and any networks or hardware, including but not limited to that provided by the School. It applies to any personal devices and other equipment that can be used to access, store or record data or media files.

"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim." *Dr Tanya Byron Safer children in a digital world: the report of the Byron Review.*

The School recognises that Web 2.0 [for example: blogs, wikis and social networking tools] encourages a new collaborative way of thinking and exploring information with considerable ease. It is important that students, parents and staff are able to identify and verify material found on the web for its own worth: they should not be so naïve to think that data is immune from being inappropriate, biased, bullying or exploitative in nature. It is not enough to impose a list of restrictions; The Hammond wishes to educate and safeguard students, parents and staff on the best use of ICT and alert them to the dangers.

Risks

Initial concern for children is largely centred on their use of social networking sites, and the possibility that they could be 'groomed' by those with a malicious intent. This is made possible by the amount of personal information that children can disclose online allowing predators to manipulate them by becoming their online friend, often hiding their true age and identity and developing close friendships by pretending to share common interests in music, personalities, sport or other activities for which children have expressed a specific liking. The huge publicity surrounding chat rooms and the decision by some leading commercial companies to close their chat rooms to children led to the focus switching to social networking applications. In some respects these are more of a problem than chat rooms, as young people share 'friend lists' and pass on contacts one to another. As instant messaging programmes allow private one to one correspondence with or without the use of webcams, they also can give even greater privacy to predators developing relationships with children online.

It is important to understand that social networking sites are public spaces where adults can also interact with children, which obviously has an implication on child safety. Whilst encouraging young people to be creative users of the internet who publish content rather than being passive consumers, there is a balance to be weighed in terms of the personal element of what is being published. The concerns are shifting from what children are ‘downloading’ in terms of content to what they are ‘uploading’ to the net. In some cases very detailed accounts of their personal lives, contact information, daily routines, photographs and videos are acting as an online shopping catalogue for those who would seek children to exploit, either sexually or for identity fraud purposes. These sites are very popular with young people as not only can they express themselves with an online personality, but they can use all the applications the site has to offer to chat and share multimedia content with others - music, photos and video clips. Unfortunately, these sites can also be the ideal platform for facilitating bullying, slander and humiliation of others. The better sites are now taking this issue seriously and ensuring that they have safety guidelines and codes of practice in place.

Cyber Bullying
With increasing new communication technologies being made available to children and young people, there will always be a potential for them becoming a victim to online bullying. Online bullying, e-bullying or cyber bullying, is defined as follows: 'the use of information and communication technologies such as email, [mobile] phone and text messages, instant messaging, defamatory personal websites and defamatory personal polling websites, to support deliberate, repeated, and hostile behaviour by an individual or a group, that is intended to harm others.'

Children and young people are keen adopters of new technologies, but this can also leave them open to the threat of online bullying. An awareness of the issues and knowledge of methods for dealing with online bullying can help reduce the risks.

Please see the Cyber Bullying section in the Anti-Bullying Policy for more support.

Social Media, Instant Messaging and Chat Rooms

Aside from the general risks of using chat rooms and instant messaging (IM) services, these services are also used by bullies. Children should be encouraged to always use moderated chat rooms, and to never give out personal information while chatting. If bullying does occur, they should not respond to messages, but should leave the chat room, and seek advice from a teacher, parent or carer. If using a moderated chat room, the system moderators should also be informed, giving as much detail as possible, so that they can take appropriate action.

Instant Messaging (IM) is a form of online chat but is private between two, or more, people. If a child is bullied or harassed by IM, the service provider should be informed giving the nickname or ID, date, time and details of the problem. The service provider will then take appropriate action which could involve a warning or disconnection from the IM service. If a child has experienced bullying in this way, it might also be worth re-registering for instant messaging with a new user ID.

Websites

Although less common, bullying via websites is now becoming an issue. Such bullying generally takes the form of websites that mock, torment, harass or are otherwise offensive, often aimed at an individual or group of people. If a child discovers a bullying website referring to them, they should immediate seek help from a teacher, parent or carer. Pages should be copied and printed from the website concerned for evidence, and the internet service provider (ISP) responsible for hosting the site should be contacted immediately. The ISP can take steps to find out who posted the site, and request that it is removed. Many ISPs will outline their procedures for dealing with reported abuse in an acceptable use policy (AUP) which can be found on their website. Additionally, many websites and forum services now provide facilities for visitors to create online votes and polls, which have been used by bullies to humiliate and embarrass their fellow students. Again, any misuse of such services should be reported to a teacher, parent or carer who should then take steps to contact the hosting website and request the removal of the poll.

Service Provision

Networked Computers
Every person using computers connected to The Hammond Network is allocated network file space to store personal work. It is not to be used for personal music, picture files or anything not related to their academic learning or work. Users will be given rights to use certain shared files, networked printers and other resources as well as internal email. Connection of personal computers to the network requires permission from the ICT Department.

Internet use in the boarding houses
There are additional e-safety rules governing the use of the Internet in the boarding houses. These e-Safety Rules help to protect boarding students and The Hammond by describing acceptable and unacceptable computer use. They complement the existing whole school ICT policy. However, a signed acknowledgement of an awareness of this boarding policy has been signed by the student and parent(s) and is held by the housemaster/mistress responsible for each house (filed within the student's personal documents).

Internet access in each of the boarding houses is provided via the use of a BT Home Hub and is directly linked to the school's filtering system via two VPNs (Virtual Private Network). Internet access is wireless and when the necessary written permissions have been received, and following an e-safety presentation, students are provided with an internet connection

Printing
Students are allowed access to most printers. When a user logs on a local printer is assigned, this printer is normally the nearest printer to the computer they log on to. The Hammond has installed print management software, which monitors all printed output. It is the responsibility of all users to ensure that the print facilities in School are used in a cost-effective manner

Students
In relation to ICT, the following are the rules by which students must adhere while at The Hammond School.

- Students must not interfere with the work of others or the system itself
- No one must create, store, transmit or cause to be transmitted material which is offensive, obscene, indecent or defamatory or which infringes the copyright of another person
- Students must not transmit any messages or prepare files that appear to originate from anyone other than themselves
- Students should NOT come into School with mobile internet connectors e.g. 'dongles'. These will be taken from the students and returned to parents at the first available opportunity.
- Students must not gain or attempt to gain unauthorised access to other student's files or facilities or services accessible via local or national networks or transmit any confidential information about the School: they must not attempt to get around service limitations placed on the network used by the School (or its agents)
- Students must not send any message internally or externally which is bullying, abusive, humiliating, hostile or intimidating.
- Students must compose any e-mail or telephone calls (or other electronic communication) with courtesy and consideration

Security
The School expects all its members to maintain high security over the information they make available on the internet by using secure sites, high privacy settings and using strong passwords.

Students must not disclose passwords to anyone and must not attempt to discover or use the passwords of others. They must take sensible precautions to avoid Internet viruses and should not access sites with age restrictions beyond their years.

Monitoring
The School reserves the right to monitor communications and general network usage in order to:

- Protect students
- Establish the existence of facts
- Prevent or detect crime
- Investigate or detect unauthorised, suspicious or inappropriate use of School ICT systems
- Ensure the effective operation of the School network and its systems

Education
The Hammond recognises that blocking and barring sites is no longer adequate. It aims to teach all students to understand why they need to behave responsibly if they are to protect themselves. We offer specific guidance on the safe use of social networking sites, which covers personal security settings.

Mobile Phones

The school considers online safety a part of both safeguarding, anti-bullying and mobile devices (see separate policies). This includes the use of cyber technology to bully, including social media, websites, mobile telephones, text messages, photographs and emails.

The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click. The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone, has been seized by a member of staff who has been formally authorised by the Principal, that staff member can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone. If an electronic device that is prohibited by the school rules has been seized and the member of staff has reasonable ground to suspect that it contains evidence in relation to an offence, they must give the device to the police as soon as it is reasonably practicable. Material on the device that is suspected to be evidence relevant to an offence, or that is a pornographic image of a child or an extreme pornographic image, should not be deleted prior to giving the device to the police.1 If a staff member finds material that they do not suspect contains evidence in relation to an offence, they can decide whether it is appropriate to delete or retain the material as evidence of a breach of school discipline.

It is evident that as well as the increased prospect of cyber bullying, mobile phones have a considerable impact of the professional life and culture of the school. The use of mobile phones during the school day has a negative impact on the social interactions of pupils, therefore, as of September 2023, it was agreed that The Hammond would ban the use of mobile phones during the school day for Lower School pupils.

Boarders will not be allowed their mobile phone on site. Boarders should leave their mobile phone at their boarding house before boarding the bus each morning. Day pupils are required to hand their mobile phone into their form tutor at 8.45am and will have them returned to them at the end of the school day at 6.00pm.

Pupils' phones will be stored in a box and locked away in the pastoral office for the day.

This policy should be read in accordance with the school Behaviour Management Policy. Any pupil who does not adhere to the policy and procedure regarding mobile phones will be sanctioned in accordance with the school Behaviour Management Policy.

The Hammond recognises the use of mobile phone technology can be beneficial to teaching and learning. Any use of mobile phones during lesson time will be at the discretion of the staff member and should only be used for educational purposes. The staff member is responsible for the collection of mobile phones and returning them to their locked location at the end of the lesson.

Young people continue to be guided as regards appropriate usage through form activities, assemblies, PSHE and other activities. School pupils are guided to know that they may not bring a mobile devices to school, but have access to mobile devices in the boarding houses. Robust filtering mechanisms are in place to prevent inappropriate material being viewed by pupils, students, or staff. Regular staff briefings, pupil and student assemblies, as well as PSHE activities are conducted regarding online safety, consolidated by follow-up emails and notes. Newsletters are created which include information regarding online safety, as well as emails to parents and guardians. All members of the school community are asked to report any breaches of the above rules by contacting a form tutor, or a member of the senior leadership team. Any unkind behaviour will be treated in the same manner as any face to face unkind behaviour is treated.

The Hammond is fully aware of the high-profile use of mobile technology, particularly access to 3G and 4G internet, in the world today. It is acknowledged that this plays a large part in the lives of our pupils and students and can have positive outcomes. However, there are some clear risks when children are able to go online.

The NSPCC state that 'the most effective filter is an educated child'. We work closely with pupils to educate them on safe use of the internet through dedicated lessons, form tutor time, PSHE drop-down days and assemblies. During the school day, the following precautions are aimed at reducing the possibility of pupils having difficulties:

- Pupils may not bring a phone to school; college students may bring a phone to school and abide by the acceptable use procedures and rules.
- During evenings, in the boarding houses, children are allowed access to their mobile devices but these are removed at bed time and locked away by Houseparents.

To support boarders, the following information is provided to the parents of boarders through our boarding handbook:

The controls you've set up on your child's device and your home broadband won't apply if they use 3G or 4G, public WiFi or log on to a friend's connection instead. Public WiFi is often available when you're out and about. But it's not always secure and can allow children to search the internet free from controls.

Some venues and businesses offer family-friendly WiFi. When you see the family-friendly WiFi symbol it means that when you connect to the WiFi there are filters in place to stop children from seeing harmful content. Talk to your child and agree with them what they can and can't do online. And if they're visiting friends or family remember that they might not have the same controls set up.

For step-by-step guides on how to set up on how to parental controls on specific mobile and broadband networks please see the link below:

https://www.internetmatters.org/parental-controls/broadband-mobile/

Staff must **not** have any current child as their 'friend' on any of the social networking sites such as Facebook, nor should they 'follow' them on other platforms such as Twitter or Instagram. This remains in place for three years following the student's transition from the school. Staff must contact children using their school email address only, and only for academic or vocational purposes. This is regularly communicated through staff briefings and INSET training. This extends to young people undertaking the degree course at The Hammond. Please see the Staff Behaviour Policy for more information.

In keeping with the guidance publication, Keeping Children Safe in Education September 2023, The Hammond has a whole school policy regarding the safe usage of the internet. Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Filter content lists are regularly updated (via www.trustedsource.org) and internet use is logged and monitored. There is a clear route for reporting and managing changes to the filtering system. Where we allow children and staff to bring their own devices, they are allowed internet access through the school network, filtering will then be applied that is consistent with school practice.

- The school has provided differentiated user-level filtering through the use of Sophos devices. These allow for different filtering levels for different ages / stages and different groups of users – staff / pupils / students.
- Children will be made aware of the importance of filtering systems and the way in which the school's works upon their induction programme.
- Mobile devices that access the school internet connection will be subject to the same filtering standards as other devices on the school systems
- If a member or staff or a child has concerns regarding the accessible content, they can contact IT Support.
- If there are any concerns regarding a particular child or member of staff, the school can monitor their internet usage and lock their account until the matter is resolved.
- Any filtering issues are reported immediately to the filtering provider, Virtue Technologies, who then manage the filtering system remotely to resolve any problems.
- If the filtering system is compromised in any way, the Sophos devices disallow connection to the source so there is no instance where children and staff can access the internet unfiltered.
- The measures above are carried out in accordance with Safeguarding and Prevent strategies in order to protect children from online threats presented by access to the internet.

Using mobile phones to harass or upset other people in any way is an offence punishable by law and by the School. This includes the use of Social Media, where you should not use language that could be calculated to incite hatred against any ethnic, religious or other minority group. Furthermore, you should be aware that derogatory language used to or about your peers or your teachers may be looked into.

Interfering with, hiding or taking someone else's mobile phone will be regarded as theft and quite possibly, bullying as well. This will be dealt with accordingly (see sanctions below).

Mobile phones, watches and smart watches are banned at all times from examination rooms.

Detail regarding the use of Mobile Devices in School

Mobile phones and, in particular, the new generation of smart phones, such as the iPhone, now include many additional functions such as an integrated camera, video recording capability, instant messaging, mobile office applications and mobile access to the internet. These allow immediate access to email, searching for information on the internet and other functions such as access to social networking sites e.g. Facebook, twitter and blogging sites.

For many young people today the ownership of a mobile phone is considered a necessary and vital part of their social life. When used creatively and responsibly the smart phone has great potential to support a pupil's learning experiences. In recent years we have had incidents of poor conduct where mobile phone use has been a feature. This is particularly difficult to address if it is an element in bullying. Bullying, intimidation and harassment are not new in society; however bullying using a mobile phone represents a new challenge for schools to manage. Parents and pupils should be clear that misuse of mobile phones will not be tolerated and any misuse will be treated as a serious breach of behaviour policy. The following are examples of misuse but are not exclusive.

'Misuse' will be at the discretion of the Principal:

- the deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience such as on social media
- bullying by text, image and email messaging
- the use of a mobile phone for 'sexting' (the deliberate taking and sending of provocative images or text messages)
- pupils posting material on social network sites with no thought to the risks to their personal reputation and sometimes with the deliberate intention of causing harm to others
- making disrespectful comments, misrepresenting events or making defamatory remarks about teachers or other pupils
- general disruption to learning caused by pupils accessing phones in lessons
- pupils phoning parents immediately following an incident so that the ability of staff to deal with an incident is compromised
- publishing photographs of vulnerable pupils, who may be on a child protection plan, where this may put them at additional risk.

Dealing with breaches

Misuse of the mobile phone policy will be dealt with using the same principles set out in the school behaviour policy, with the response being proportionate to the severity of the misuse. Pupils are aware that serious misuse lead to the imposition of other sanctions up to and including exclusion from school. If the offence is serious, it will be reported to the Police.

The Hammond uses a procedure when a mobile phone has been confiscated and is not returned to the pupil/student after removal. The Hammond will ensure that the confiscation is correctly recorded and that the phone is kept securely. Where it is deemed necessary to examine the contents of a mobile phone this will be done by a designated member of staff. The action will be properly recorded in case it later becomes evidence of criminal activity. The record will include the time, who was present and what is found.

Rules for the Acceptable Use of a mobile phone in school by pupils/students.

Day pupils are allowed to bring mobile phones into school for the purposes of emergency contact if travelling alone to or from school, but they must be handed in at the start of the working day. If they choose to do so it is on the understanding that they agree with the following limitations on its use, namely:

· Mobile phones must be switched off and handed in to their form tutor at 8.45am to be returned at 6.00pm. It is not acceptable for phones merely to be put on silent or pager mode.

· No pupil may take a mobile phone into a room or other area where examinations are being held.

· If asked to do so, content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher

The Hammond will not take responsibility for the loss, theft or damage to any mobile device; the pupil/student brings their mobile device at their own risk.

Unacceptable use

The Hammond will consider any of the following to be unacceptable use of the mobile phone and a serious breach of the school's behaviour policy resulting in sanctions being taken.

- Photographing or filming staff or other pupils/students without their knowledge or permission
- Photographing or filming in toilets, changing rooms and similar areas
- Using a mobile phone out of the classroom.
- Using a mobile phone to contact parents in such a way that it impedes the positive dealing of the incident by a member of staff.
- Bullying, harassing or intimidating staff or pupils/students by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites
- Refusing to switch a phone off or handing over the phone at the request of a member of staff

- Using the mobile phone outside school hours to intimidate or upset staff and pupils/students will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time
- Using a mobile phone outside school hours in such as way that it undermines the stability of the school and compromises its ability to fulfil safeguarding duties.

Sanctions

Pupils/students and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines, following the schools behaviour policy. In addition:

• pupils/students and their parents should be very clear that the school is within its rights to confiscate the phone where the guidelines have been breached. Using the mobile phone outside school hours to intimidate or upset staff and pupils or undermine the stability of the school in any way will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

• If a phone is confiscated, school will make it clear for how long this will be and the procedure to be followed for its return.

• Pupils/students should be aware that the police will be informed if there is a serious misuse of the mobile phone where criminal activity is suspected

• If a pupil commits an act which causes serious harassment, alarm or distress to another pupil or member of staff the ultimate sanction may be permanent exclusion. School will consider the impact on the victim of the act in deciding the sanction.

Confiscation procedure

If a mobile phone is confiscated then:

• at the discretion of the teacher the mobile phone will be returned to the Houseparents (if a boarder) or to the pupil/student at the end of the day

• or the pupil will be informed that the phone can be collected at the end of school day from the nominated senior member of staff

• the confiscation will be recorded in Class Charts for monitoring purposes

• school will ensure that confiscated equipment is stored in such a way that it is returned to the correct person

• in the case of repeated or serious misuse the phone will only be returned to a parent/carer who will be required to visit the school by appointment to collect the phone.

This may be at the end of a week, a half term or longer. At the discretion of the Principal the phone may be returned to the pupil at the end of the confiscation period.

• where a pupil/student persistently breaches the expectations, following a clear warning, the Principal may impose an outright ban from bringing a mobile phone to school. This may be a fixed period or permanent ban.

Where the phone has been used for an unacceptable purpose

• The Principal or a designated staff member will have the right to view files stored in confiscated equipment and if necessary seek the cooperation of parents in deleting any files which are in clear breach of these guidelines unless they are being preserved as evidence.

• If required evidence of the offence or suspected offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen

• School will consider whether an incident should be reported to the safeguarding local partners, including the Police.

• The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator or the victim which needs further investigation.

Cameras

IMPORTANT
The use of cameras, including those on mobile phones, are not permitted in lessons, plays or concerts or any other School activity where they could justifiably be regarded as an interference or intrusion. Care must also be taken in students' bedrooms or dormitories where they are be used in a way that could justifiably be regarded as intrusive or embarrassing. Staff may take and use images of students purely for work purposes and where possible such images will not be stored on personal electronic devices.

Parents agree in writing to The Hammond using images of students for promotional and web material provided the students are not named and the images are stored securely. It is recognised that when taking photographs of School events some images may capture students other than the intended subject. Parents/guardians should use any personal images with careful consideration for those in the picture and should not publish them on external websites. Please also see the Data Protection Policy.

Sanctions

In the event of any breach of the policy, appropriate sanctions are imposed in line with the School's policy: this may include the restriction of a student’s access to the School network, the confiscation of any personal or shared devices being used to infringe these or any wider School rules. More serious sanctions will include suspension or expulsion. If the breach is of a criminal nature, the Police and local safeguarding partners may be involved. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP).

Students and parents sign a contract agreeing to Acceptable Use of ICT at The Hammond School. The likely sanctions for minor breaches of the policy are detailed below:

- 1st offence – confiscation of equipment for 1 day or until the end of the day for day pupils and to be handed in the next day to continue the sanction.
- 2nd offence – confiscation of equipment and loss of access privileges for 48 hours
- 3rd offence – confiscation and loss of access privileges for longer period, to be determined.

Confiscated equipment must be returned to the Director of Boarding or School Office where it will be safely stored before returning to the students or parents.

Please Note: - The school cannot be held responsible for loss or damage to any mobile device brought into school and used by a pupil/student/member of staff.

Please also see: - Safeguarding Policy, Anti-Bullying Policy, Behaviour Management Policy, and Exclusion Policy.

Policy Details

This Page Should Not Be Published

Document Owner:	J ROSCOE
Document Input:	SLT
Document Sources:	DFE
First Created Date:	JULY 2022
Last Update Date:	AUGUST 2023
File Location of Original Policy:	SHAREPOINT

Approver	BOARDING AND SAFEGUARDING COMMITTEE
Role	BOARD OF DIRECTORS
Last Approval Date	AUGUST 2023
Next Review Date	AUGUST 2024