Flawwood Hawwood Hawwood

STATEMENT REGARDING THE USE OF MOBILE TECHNOLOGY

2023-24

THE HAMMOND SCHOOL LTD., MANNINGS LANE, CHESTER, CH2 4ES Telephone: 01244 305350 | Web: <u>www.thehammondschool.co.uk</u> | Email: <u>contact@thehammondschool.co.uk</u>

The Hammond School Limited is registered in England and Wales Number 838325. Registered office is above. Charity Number 1022427 incorporating the Betty Hassall Foundation. The school is accredited by the I.S.A and C.D.E.T. and is a member of the B.S.A and I.S.I.

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.

The Hammond provides a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. The Hammond understands the importance of ensuring the right people are working together and using their professional expertise to make informed decisions.

The Hammond seeks to achieve this by:

- Nominating the DSL (as a member of the senior leadership team) and the safeguarding Director, to be responsible for ensuring these standards are met
- the roles and responsibilities of staff and third parties, for example, external service provide, are clearly identified through regular meetings.

The DSL is responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why

- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

The DSL takes lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

The Board of Directors has overall strategic responsibility for meeting the standard. They make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.

The review should be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible director. The results of the online safety review should be recorded for reference and made available to those entitled to inspect that information.

As of September 2023, The Hammond removed the ability of pupils to bring and use mobile devices in school (boarders are able to access mobile devices withing boarding time). College students are allowed to bring and use mobile devices at college, providing they abide by the acceptable use procedures. 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 PSCHE 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.

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. 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 Red 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 the Head of IT.
- 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 Red devices disallow connection to the internet 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.
- The nature of this filtering system does not allow for connections to social media accounts on the school's internet provision. This negates the threat of online radicalisation via the use of social media.

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.

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 and Exclusion Policy.

Social Networking Sites and Internet Safety, Online Safety

As The Hammond begins to increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. The Hammond ensures that appropriate filters and monitoring systems are in place. For more information, please see the Internet Filtering Policy.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation, radicalisation, sexual predation: technology often provides the platform that facilitates harm. The Hammond ensures an effective approach to online safety to protect and educate the whole community and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

There are three four areas of risk:

Content: being exposed to illegal, inappropriate or harmful material, for example pornography, fake news, racist or radical and extremist views.

Contact: being subjected to harmful online interaction with other users, for example commercial advertising as well as adults posing as children or young adults.

Conduct: personal online behaviour that increases the likelihood or, or causes, harm, for example making, sending and receiving explicit images, or online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If a Hammond member of staff feels pupils, students or staff are at risk they are asked report to the Anti-Phishing Working Group <u>https://apwg.org/</u>

STATEMENT REGARDING THE USE OF MOBILE TECHNOLOGY 2022-23

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