## 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.

**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**
Mobile phones are banned from The Hammond during the school day. Boarding students are asked to leave their phones at the boarding houses of a morning. Day pupils may have a mobile phone in their bag, but this must be switched off and not used. This is to enable those students to arrange transport and to travel home safely and for communication in an emergency.

If a student brings/uses a mobile telephone on the school site the phone will be confiscated and passed to the main office. Boarding pupils’ phones will be returned to boarding staff. Day pupils may collect their phone from the office at the end of the day.

For day pupils who are ‘repeat offenders’, parents will be required to come in person to reclaim their child’s mobile device from the school office. The rules above apply to the use of headphones and ear pieces.

If a student is feeling unwell they should first contact the school office where staff will contact parents if necessary.

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 Children's Board (LSCB) 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 Head of Boarding or Reception 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 student.

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