PRAESTAT OPES SAPIENTIA

HAMPTON SCHOOL

ESafety Policy

1. Development

This ESafety policy has been developed by Jack Talman (JHT), the ESafety Officer, along with Owen Morris (JOM) (Deputy Head, Pastoral and Designated Safeguarding Lead) and Pippa Message (PZM) (Deputy Head, ICT).

2. Monitoring / Review

The ESafety Officer & SMT will review the policy annually. The policy is required to be reviewed and updated annually as the technological environment changes rapidly. Technological developments such as the internet and other forms of electronic communication have great educational and social benefits but can also be used to harm others. Hampton School is committed to working with parents and pupils to address the issues that are presented in this area.

3. Scope

This policy applies to all members of the School community (including staff, pupils, parents, visitors) who have access to and are users of School ICT systems, both in and out of the School.

The School will deal with ESafety incidents in accordance with the procedures outlined in this policy and in associated School policies, such as the Safeguarding and Anti-Bullying policies. The School will inform parents of incidents of inappropriate ESafety behaviour that take place in or out of School.

When necessary, the School will inform the police or Achieving For Children (Richmond and Kingston). Procedures in the Safeguarding Policy outline this in more detail.

4. Other Relevant Policies

This policy should be read in conjunction with the following other School policies:

- **Safeguarding Policy** (which makes particular reference to ESafety and the three "areas of risk" outlined in *Keeping Children Safe in Education* (KCSiE) 2016 – online conduct, contact & conduct);
- **Anti-Bullying Policy** (which contains particular reference to Cyber-bullying and possible examples of this);
- **Staff Behaviour Policy** (which contains particularly relevant sections on staff communication with pupils, staff internet use, staff use of social networks;
- **Pupil ICT Acceptable Use Policy (available on Canvas and Firefly)**
- **Data Protection Policy;**

Date updated	October 2017	Date ratified by Governors	December 2017
Date of next review	October 2018	Reason for Review	Annual Review

Definition of “Inappropriate” in a digital context: School policy documents, agreements and guidelines refer to 'inappropriate' use of School resources or 'inappropriate' behaviour. In these policies, a website or activity is 'inappropriate' if it is:

- Illegal
- Obscene
- Discriminatory
- Defamatory
- Homophobic
- Pornographic or of a sexual nature
- Racist
- Negatively stereotyping
- Fraudulent
- Threatening
- Abusive
- Threatening to School security

5. ESafety

Mobile devices and computers are a source of education, communication and entertainment. However, some adults and young people may use these technologies to harm children and we are aware of the Safeguarding concerns linked to ESafety. *KCSiE2016* outlines three areas of risk:

(i) online content (being exposed to harmful material);
(ii) contact (being subjected to harmful interaction with others online); and
(iii) conduct (personal online behaviour that increase the likelihood of, or causes, harm).

The School will take all reasonable measures to:

a) Educate pupils, and educate and train staff and parents about ESafety:

The School reinforces Internet safety messages to all pupils at regular intervals and at an age-appropriate level through PSHE lessons, assemblies and by inviting in external organisations/experts. Issues covered include the following:

- safe and appropriate use of social networking sites;
- the issues surrounding excessive use of games consoles, Internet gaming sites, mobile phones (especially texting) and social networking or messaging facilities;
- the sending of inappropriate photos via mobile phone or the Internet;
- the dangers of illegal and harmful substances sold online;
- the effect on pupils’ wellbeing and self-image of social media and other messages that they may get from online activity;
- the effect of internet pornography on pupils’ self-image and their relationships with others

We ensure all pupils and members of staff are informed of the School’s ICT Acceptable Use Policies [Staff & Pupil] , which explain their responsibility for safe and appropriate use of the School’s computer systems.

Advice on cyber safety and cyber issues is given to parents from time-to-time at Year Group Pastoral Forums for parents, at Parents’ Evenings and on other occasions.

b) The School has also put in place in place appropriate filters and monitoring systems to protect children, while being mindful not to place unnecessary restrictions on the learning.
c) The appropriate School disciplinary procedures will be followed in relation to any incident of misuse of ICT equipment or websites or of cyber bullying. Clear advice is given to pupils regarding the appropriate use of technology in School. The School reserves the right to take action - even when the offence is committed outside of School - if it harms members of our community or brings the School into disrepute.
d) The School has appointed an ESafety Officer (JHT, also Head of PSHE) to coordinate ESafety measures and to work closely with the Deputy Heads over ESafety matters. ESafety incidents will be monitored via an ESafety log.

6. Education – Pupils

ESafety should be a focus of all areas of the curriculum and staff should reinforce ESafety messages across the curriculum. The ESafety curriculum should be broad, relevant and provide progression, and will be provided in the following ways:

- An ESafety curriculum is provided as part of PSHE lessons and is regularly revisited *(see below*).
- Key ESafety messages are reinforced as part of a planned programme of whole school and individual year group assemblies.
- Pupils are taught to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
- Pupils are helped to understand the need for the ICT Acceptable Use Policy and encouraged to adopt safe and responsible use of the digital world both within and outside of school.
- Pupils are helped to understand the benefits and risks associated with social media, online posting and messaging.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

ESafety Education in PSHE

Every form begins the year with a discussion of expectations of behaviour and cyber safety regarding

Bring Your Own Device (BYOD) and iPads. This is also specifically addressed in PHSE lessons at the following times:

First Year (Year 7)

- 3 lessons including talk from DAUK – Digital Awareness UK

Second Year (Year 8)

- 4 lessons, boys produce presentations on issues relating to cyber-safety
- Sex and Relationship Education talk includes reference to cyber-safety
- Lesson on self-esteem considers cyber-related issues
- Personal Safety Day addresses safety with regard to expensive devices

Third Year (Year 9)

- 3 lessons on cyber safety issues
- Lesson on self-esteem, body image considers cyber related issues

- Cyber related issues covered extensively in SRE programme

Fourth Year (Year 10)

- 3 lessons on cyber safety
- 2 SRE talks focus highly on cyber related issues
- Screen Time talk

Lower Sixth (Year 12)

- Cyber-Safety talk

Upper Sixth (Year 13)

- Cyber-Safety Talk & Follow Up lesson

7. Education – Parents

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviour.

Advice on cyber safety and cyber issues is given to parents from time-to-time at Year Group Pastoral Forums for parents, at Parents' Evenings and on other occasions.

This advice is drawn from recommendations made by the Child Exploitation and Online Protection Centre (CEOP):

- Make yourself aware of the amount of time your child is using the Internet, chat facilities, games consoles and their mobile phones and whether this is excessive
- Consider carefully the location of the computer or laptop and whether your child would be better using it in a family area of the home
- Search on Google and other search engines for your child's name and any online usernames they use. This is a valuable exercise for you and them to see exactly how much other people can see about them with very little difficulty
- Consider installing Internet monitoring software on home computers
- Talk to your child; both about the dangers or the Internet, but also about their general usage – be interested in what they are doing and keep a dialogue open so they feel able to talk to you if they do experience problems
- Ask your child to (or help them) set up appropriate privacy settings on Facebook (please contact the School if you need help or advice in this area)

8. Education and Training – Staff

Staff receive training on INSET days as well as updates during Tuesday briefings on IT and E-Safety issues. Firefly contains further advice. The Staff Behaviour Policy and Staff Handbook also contains sections with advice on staff communication with pupils, staff internet use and staff use of social networks.

Since September 2015, all teachers have completed the NSPCC Online ESafety course.

9. Digital Council & Digital Ambassadors

The school's digital council meets regularly with the relevant Deputy Head (PZM) and IT staff. This is a student body who are consulted on cyber issues and includes boys from all year groups. Some

members of the Digital Council are also 'Digital Ambassadors' who take a particular interest in E-Safety and developing ways to help their peers to stay safe online.

10. Filtering and Monitoring

The School network uses filtering software, which amongst other things restricts access to social networking and gaming sites. Filtering is age-appropriate. In addition, there is a process of monitoring of online activity using the School network.

As part of its Prevent Duty, the School has put in place filtering and monitoring is in place to ensure children are safe from terrorist and extremist material when accessing the internet in school.

More information on the school filter and monitoring is in the **Safeguarding Policy**.

11. Behaviour and Anti-Bullying

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, and they can be escalated to safeguarding concerns.

We follow the appropriate School disciplinary procedures in relation to any incident of misuse of ICT equipment or websites or of cyber bullying. The School reserves the right to take action - even when the offence is committed outside of School - if it harms members of our community or brings the School into disrepute.

Cyber bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, against a victim who cannot easily defend him/herself. It is sometimes also known as 'online abuse' as the term cyber-bullying can become trivialised through overuse. Mobile, Internet and wireless technologies have increased the pace of communication and brought benefits to users worldwide. Unfortunately, however, their popularity provides the opportunity for misuse through cyber bullying.

Cyber bullying includes: Text message bullying; picture/video bullying via mobile phone cameras; phone call bullying via mobile phone; email bullying; chat room or social network bullying; bullying through instant messaging; bullying via websites; bullying via gaming platforms.

Ways to keep yourself and others safe include:

- Do not post items/information that is personal – keep information general.
- Think carefully about posting pictures online – once it is there, anyone can see it or use it.
- Do not share your passwords – keep your personal information private!
- Never meet up with someone you meet online without a responsible adult – you do not really know who they are!
- Try to think carefully before you write things online – people can get the wrong end of the stick.
- Respect other people's views – just because you do not agree with them, it does not mean you have to be rude or abusive.

What can you do?

- Tell someone you trust.
- Report any cyberbullying, even if it is not happening to you.
- Never respond/retaliate as it could make matters worse.
- Block the cyberbullies from contacting you.

- Save and print any bullying messages, posts, pictures or videos that you receive or see online.
- Make a note of the dates and times they are received.
- Keep your passwords private.
- Don't post any personal information or pictures online

Sexting and revenge porn are taken particularly seriously and boys are educated about the dangers and possible consequences of these acts through PSHE lessons.

Cyber bullying is explicitly referred to in Hampton School's Anti-Bullying Policy. The School's expectations of pupils in this area are clearly set out in the School Code, which is printed each term in every boy's yellow School calendar. School Assemblies and PHSE lessons are also used to update pupils on relevant cyber issues.

12. Use of the Internet, e-mail and other forms of digital technology;

The School views very seriously any use of the Internet, e-mail and any other digital media or technology so as to conflict in any way with the School Code, AUP, brings the School's name into disrepute, to cause hurt or distress to others (cyber bullying), or to have a negative impact on the School community in any way. Any student found to have misused the above technology in such a manner faces losing his place at Hampton School. The School's view applies whether or not a student is on the School premises, in the care of the School, wearing School uniform or on a School trip.

The School is able to monitor students' use of School computers and the School network to access external websites.

The school expects the following from pupils when using the school system:

All ICT and Internet activity must be appropriate to the student's education.

- Access should only be made via the authorised password, which must not be made available to any other person.
- Activity that threatens the integrity of the School ICT systems, or activity which attacks or corrupts other systems, is strictly forbidden.
- E-mail can only be used for legitimate School-based purposes.
- Students must understand that the network is monitored constantly and infringements will be reported. Students contravening these guidelines will be removed immediately from the network and will be subject to the School's discipline code and ICT sanctions.
- Use for purchasing goods and services or advertising on the Internet is strictly forbidden.
- Use for personal financial gain, gambling, political purpose, incitement of terrorism, extremism or radicalisation is strictly forbidden.
- Copyright of materials must be respected. If information is obtained from the Internet, any directly quoted material must be clearly specified and its source listed in the bibliography. Copyright protected media files must not be downloaded or stored on the Schools systems unless they are covered by the ERA Licensing Scheme.
- Use of the network to create, distribute, store or access inappropriate matter, such as pornographic, racist or offensive material, is strictly forbidden.
- Students must exercise discernment and report inappropriate material.
- Programme files must not be downloaded or installed from an external source and must not be run from a USB data stick or other external storage device.

- Consideration towards other students and staff using ICT areas is essential: e.g., sound without headphones is not acceptable because it disrupts the study of others.

13. Use of iPads, devices and mobile phones in school

During the School day boys are strictly prohibited from using iPhones or other smart phones, laptop dongles or any other means to access the Internet directly, i.e. bypassing the School's wireless network, filtering and monitoring systems, and they must abide by the School's AUP. All devices should be fully charged at home each evening and charging cables should not be brought into School. Devices are for personal use only and must not be shared with other pupils. Failure to follow these rules is likely to result in their confiscation and a possible sanction. Boys bringing to School mobile phones, Smart phones, iPads or other tablet computers, portable music and games systems or any other electronic equipment do so at their own risk.

i. iPads

iPads (or other tablet computers) may only be used in school for educational activities and with the explicit permission of a teacher or other member of staff. Devices must be brought to all lessons, but should be switched to "standby" or "silent" modes and remain in bags unless a teacher instructs otherwise. They should be transported between lessons in school bags, and kept in lockers when unattended. Devices may not be used in Form rooms or at other locations around the School site before school, at morning break time, or at lunchtime unless with the explicit permission of a member of staff. Failure to follow these regulations is likely to result in a sanction.

ii. Mobile Phones

Boys in the First to Third Year may keep their mobile phones on their person, at their own risk, but they must be switched off or on the "silent" or "standby" setting and must not be used during School hours unless with a teacher's explicit permission. Failure to observe these rules may attract a detention.

Boys in the Fourth Year and above only may use mobile phones to access the School's wireless network during break and lunch times or during their study periods. Such devices must not be used, at any time, in the Dining Hall, when moving about the School buildings or in the corridors; failure to observe this rule is likely to result in confiscation of the device and a possible sanction. Access to the wireless network using such devices during lesson times by any boy must only be under the direction of and with the explicit permission of the subject teacher.

The recording of audio or video clips or the taking of photographs with any device (including mobile phones) is strictly forbidden during the School day, whether on or off the School premises, when travelling to and from School or on a School activity or trip, unless permission has explicitly been given by a Head of Year, one of the Deputy Heads or the teacher in charge of the School activity or trip.

iii. Confiscation and Searching of devices

An electronic device such as a mobile phone or a tablet computer may be confiscated in appropriate circumstances in accordance with the Behaviour, Rewards, Sanctions, Discipline Exclusions Policy. If there is good reason to suspect that the device has been, or could be used to cause harm, to disrupt teaching or break school rules, any data or files on the device may be

searched and, where appropriate, data or files may be erased before the device is returned to its owner.

14. Sexting

Sexting has been defined as 'Youth produced sexual imagery': it involves children sharing images that they, or another child, have created of themselves. A child in this context means anyone under the age of 18. 'Imagery' covers both still photos and moving videos which are increasingly common. Boys and parents are educated in talks from outside speakers and by staff through PSHE on the particular dangers of sexting and revenge porn. As well as discussing the moral and social issues surrounding these a particular focus on the legal consequences of engaging in these activities is given. This includes reference to recent advice on schools and police on how to deal with sexting.

When the School becomes aware of a sexting incident, it will follow the procedures and guidance as set out in Sexting in schools and colleges: responding to incidents and safeguarding young people (UKCCIS). If a member of staff becomes aware of a sexting incident, then they must report it to the Designated Safeguarding Lead or Designated Safeguarding Officer. The Designated Safeguarding Lead will usually interview the children involved (if appropriate). Parents will usually be informed at an early stage and involved in the process (unless there is good reason to believe that involving parents would put the child at risk of harm). At any point in the process if there is a concern a child has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately. UKCCIS provides criteria for when the police and social services should be contacted. The School's sanction system will also be used depending on circumstances (refer to the School Code and the Behaviour, Sanctions, Rewards, Discipline and Exclusions Policy which refer to sexual misconduct and the possession and supply of indecent imagery).

15. ESafety: Safeguarding & "Prevent"

The School recognises that being online presents many potential safeguarding issues. Boys are educated about these in PSHE lessons and in other forums when appropriate. Staff receive regular Safeguarding training. When E-Safety issues are found to have become safeguarding issues the re

As part of the School's **"Prevent duty"** the issue of extremist or terrorist material on the internet is covered in PSHE lessons. The School's filtering software also ensures children are safe from accessing terrorist or extremist material when accessing the internet in School.

The School's **Safeguarding Policy** explains how the school addresses these issues.