E-Safety Policy

This policy is applicable to all pupils, including those in EYFS.

This policy should be read in conjunction with the Acceptable Internet Use Policies for Pupils and for Staff (attached as Appendices) and the Safeguarding Policy.

Background

Digital technologies are integral to the lives of all children at St Hugh's, including those in EYFS, both in and out of school. The technologies, such a as websites, learning platforms, blogs, social media and online gaming are powerful and exciting, they can stimulate learning and creativity and much of their use is entirely appropriate. However, these opportunities come with risks and it is essential that children use these technologies safely.

The responsibility for setting and conveying the standards that children are expected to follow when using media and information resources, is one that is shared with parents and guardians. We believe that the combination of safeguarding, communication with parents and fostering a responsible attitude amongst the pupils will provide the best opportunity to protect the pupils.

We expect all pupils and staff to treat each other online with respect, consideration and good manners.

We understand the responsibility to educate our pupils on E-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The Aims of the Policy are:

- To ensure that pupils are educated about E-Safety issues & appropriate behaviours in order that they remain safe and legal online
- To help pupils develop critical thinking skills to reflect and enable them to keep themselves safe online
- To keep personal data and information secure
- To help pupils make the right choices in their use of social media and online gaming
- To minimise the risk of pupils accessing and sharing inappropriate content

E-Safety in the Curriculum
Children are taught:

- to stay safe when using the internet both in school and out of school
- to be critically aware of content they access online
- how to recognise suspicious, bullying or extremist behaviour
- how to mitigate the risk to themselves and their peers
- how to behave responsibly and the consequences if they fail to do so
- how to report cyber bullying or incidents that make them feel uncomfortable, under threat
- how the school will respond to misuse

Specific lessons on E-Safety are the responsibility of Heads of PSHEE and Digital Learning and Development and are taught through these subject lessons and through visiting professionals. However, all staff have a responsibility to be vigilant, to understand the risks and to educate pupils as appropriate about E-Safety when using modern technology and to encourage the pupils to build their resilience to protect themselves and their peers through education and information. All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas and ensure that they are adequately informed with up to date areas of concern. The E-Learning team will endeavour to keep staff updated as well.

Age-appropriate systems are in place to keep the E-Safety message high profile. Messages and posters are displayed and staff remind pupils of high expectations in academic lessons, assemblies and extra-curricular sessions across curriculum and year groups.

Older children are taught about their online reputation and how this can have an impact, negative or positive, beyond their life at school.

An E-Safety week is held each year for Y5-8 children which highlights E-Safety throughout the curriculum, to raise the profile and importance of individual and collective safety and responsibility. Furthermore, from Pre-Prep to Upper School we organise pupil and parent education sessions on E-Safety, which are currently delivered by Childnet.

Staff should always preview recommended sites, online software and apps before using them with children.

Statement on Pupils with SEND
The School recognises that pupils with SEN may have an increased vulnerability to risk online, especially those with language and communication difficulties, or social communication difficulties. We are also aware that some SEN pupils will be using a school laptop or ipad as their normal way of working in Upper School. Staff need to be vigilant to ensure that these are kept up to date with the support of the IT department with regards to school-wide E-safety measures.

Communicating about E-Safety with Parents

Annual E-Safety workshops are run by Childnet for children of all ages and their parents to promote the importance of E-Safety both in and outside school. The school also sends regular updates to parents in the weekly newsletter and in occasional advisory letters.

Safeguarding

In order to minimise the potential of pupils being exposed to upsetting, offensive or otherwise inappropriate material online, the following measures have been adopted. However, due to the global scale and linked nature of the internet, it is impossible to guarantee that such material will not appear on a computer screen.

- We have a flexible firewall and filtering system (Lightspeed) intended to prevent access to inappropriate material for children.
- Pop-up advertisements are blocked
- Securus logs pupils browsing histories to provide a record of site visited.
- Pupils' access to the internet is routed through Lightspeed to filter their internet access.
- Access to social networking at school is prohibited for children via the network
- Anti-virus software is installed on all St Hugh's PCs and laptops.
- Copies of the Rules for Responsible Internet Use are displayed in areas with computers
- Computer use is monitored by Securus which applies key word policies and filters as well as identifying possible risk through key word libraries.

Any personal laptops brought in from home should only be given access to the School's GUEST wifi code through the ICT department, to ensure that the school's safety protocols will be in place.

Internet Misuse and the Reporting of Incidents

In the case of ICT or internet misuse, the Headmaster, Deputy Head or Assistant Head (Pastoral) will implement the measures stated in the Behaviour for Learning Policy.

This policy identifies procedures that will deal with offences, although each case is reviewed individually and the severity of the incident and the age of the pupil(s) taken into consideration. All staff are obliged to report and record any such incidents. Any complaints relating to E-Safety must follow the school's Complaints Procedure.

The safe use of digital and video images

Digital imaging technologies have significant benefits to learning. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may remain available on the internet for ever and may cause harm or embarrassment in the short or longer term. In addition, the images could provide opportunities for cyberbullying, stalking or grooming.

Staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images in ICT and PSHEE lessons.

For more detailed information, please refer to the Taking, Storing and Using Images of Children Policy. However, with the exception of use for the school's private Twitter groups (see section on Twitter), mobile phones should not generally be used to take photographs of the children. Should it be necessary to do so, and where a school device is not available, then the image/s should be transferred to the school network and deleted as soon as is possible and within 24 hours from the device and all copies in personal cloud storage removed. School cameras are available and should be used where possible. Mobile phones are not permitted in the EYFS setting nor by anyone coming into contact with the EYFS.

The use of Mobile devices (Pupils)

Mobile phones are only allowed for weekly boarders between the hours of 4.45pm and 5.30pm and then from 7.30pm until 8pm when they are handed back to the house parents. They are not allowed in dorms and the boarding house has clear rules about appropriate use. Please see the Mobile Phone Acceptable Use Policy for Boarding Pupils for more information.

The use of Mobile devices (Staff)

Staff, including those working in EYFS, should avoid using their mobile phones or personal cameras to take pictures of pupils but should use school devices wherever possible. For guidance on the use of Twitter, see the separate section. Unless in EYFS where it is not permitted, if a photo is taken using a personal phone then the photo should be deleted within 24 hours (see above).

Staff should not give their personal mobile phone numbers or email addresses to pupils, nor should they communicate with them by text message, social media or personal email. If they need to speak to a pupil by telephone, they should use one of the school's telephones and email using the school system. The group leader on all trips and visits involving an overnight stay should take a school mobile phone with him/her and may ask the pupils for their mobile numbers before allowing them out in small, unsupervised groups. The school mobiles should be used for any contact with pupils that may be necessary. The group leader will delete any record of pupils' mobile phone numbers at the end of the trip or visit and should ensure that pupils delete any staff numbers that they may have acquired during the trip.

Social networking and personal publishing

The school Social Media accounts are all private. Parents must request access to follow the accounts and this is then authorised by a designated member of staff. The privacy settings are set to ensure no one other than an authorised person has permission to view tweets and images.

When taking a photo or video and uploading it to Social Media, the member of staff doing so must immediately delete the image/video from their phone and any associated cloud account.

The management of Email

The following disclaimer is added to all emails sent via the school server:

This email and its attachments may be confidential and are intended solely for the use of the individual to whom it is addressed. Any distribution, copying or use of this communication or the information in it without the authority of the School, is strictly prohibited. Please immediately contact the sender should this message have been incorrectly transmitted. Please note that any views or opinions expressed in this message are those of the individual sender, except where the sender, with authority, states them to be the views of St Hugh's school.

E-Safety Roles and Responsibilities:

- The Governing Body has overall responsibility for safeguarding procedures within school which are delegated on a day to day basis to the Headmaster.
- The Headmaster has overall responsibility for the safety and welfare of members of the school community.
- The Headmaster delegates day to day responsibility for the online safety of pupils to the Designated Safeguarding Lead, the Assistant Head (Pastoral), the PLT, the Head of Digital Learning and Development and the E-Learning Group.
- The E-Learning Group has responsibility for keeping up to date with E-Safety developments, issues and guidance; leading the IT risk assessment; advising school staff on the appropriate use of school technology
- All staff have individual responsibilities to safeguard pupils within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- The E-Learning Group will monitor emerging technologies and make recommendations to the SLT and PLT of any changes to this policy.
- The maintenance of this policy rests with the DSL, PLT and E-Learning Group.

Monitoring and Evaluating this policy

- This policy will be evaluated at least annually by the E-Learning Group, PLT and DSL and by the Compliance Review Committee.
- Concero will monitor the effectiveness of site security and report to the Bursar and E-Learning Group termly.
- The DSL and Head of Digital Learning and Development will update the SLT of changes to legislation and good practice at least termly.
- The E-Learning Group will use the School Online Safety review Tool annually to assess progress and identify areas for improvement. (This is produced by the South West Grid for learning Ref: www.360safe.org.uk

Date last reviewed: April 2020
Reviewed by: SLT and Head of Digital Learning and Development
Date of next review: April 2021

Websites:

https://www.ceop.police.uk/safety-centre/

https://www.thinkuknow.co.uk/

https://www.saferinternet.org.uk/

https://www.childnet.com/