ST HUGH'S
OXFORDSHIRE

E-Safety Policy

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

This policy should be read in conjunction with St Hugh's policies on Anti-bullying, Acceptable Internet Use Policies for Pupils and for Staff, Behaviour for Learning, Staff Code of Conduct, Staff Handbook, Data Protection Policy, Privacy Policy, Taking, Storing and Using Images of Children Policy, Storage and Retention of Data Policy, Searches Policy, Safeguarding Policy & SEND Policy, together with the Pupil Code of Conduct and Golden Rules.

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 Aim of the Policy is:

- To ensure that pupils are educated pupils 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

- To keep personal data and information secure

- To help pupils make the right choices in their use of social media do online gaming

- To minimise the risks of pupils or staff handling sensitive information.

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 PSHE and ICT 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 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 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 & NSPCC for both pupils and children of all ages to promote the importance of E-Safety both in and outside school. The school also sends regular updates to parents and 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 IT department, to ensure that the school's safety protocols will be in place.

Internet Misuse and the Reporting of Incidents

In the case of IT 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 should educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.

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 photograph should be deleted with 24 hours from the device and all copies in the cloud 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 7.45pm until bedtime 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.

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 has four private Twitter accounts: @sthughs (for trips); @sthughsdrama; @sthughssport; and @sthughsboarding. In each case parents have to request access to join the group and then this is 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 of video and uploading it to Twitter, the member of staff doing so must immediately delete the image/video from their phone and any associated cloud account.

A policy on the use of Twitter is issued to staff which makes clear how it should be used safely.

The management of Email

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

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 IT 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 annually.
- The Network Manager will monitor the effectiveness of site security and report to the Bursar and E-Learning Group termly.
- The DSL and Network Manager 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 areas for improvement. (This is produced by the South West Grid for learning Ref: www.360safe.org.uk

Date last reviewed: September 2018

Date of next review: November 2019

Pupil IT Acceptable Use Policy - Rules for Responsible Network Use

The following rules cover use of all forms of IT at St Hugh's. They are displayed in IT areas and all pupils agree to follow these rules each time they log on to the St Hugh's network. They help you to keep safe and respectful of others when using IT in school. The Code of Conduct and Golden Rules also apply when you are logged onto the network.

Our Network

- Use the St Hugh's IT network for school and education-based purposes only
- Use the St Hugh's IT network only when you have permission to do so from a member of staff
- Access the network using only your own username and password and keep these private
- Open, edit and delete only your own documents and files
- Do not download or install programs or applications to the school's IT equipment
- Understand that the school monitors your IT use at all times
- Do not connect your own mobile device to the network without the permission of the Head of IT

Using the Internet

- Use the St Hugh's internet for school and education-based purposes only
- Use the St Hugh's internet only when you have permission to do so from a member of staff
- Behave in a responsible way when online –are your actions true, helpful, necessary and kind?
- Report any unpleasant or inappropriate material to an adult immediately
- Access to chat rooms or social networking sites is NOT allowed
- Never share personal details about yourself with anyone over the internet
- Respect the copyright of digital material
- Understand that the school monitors your Internet use and the sites that you visit and that your internet access is filtered at all times

Use of IT Equipment

- Use St Hugh's IT equipment only when you have permission to do so from a member of staff
- Take good care of all IT hardware at all times

- Do not eat or drink near IT equipment
- Sit comfortably when using IT equipment: adjust the chair and/or monitor height if necessary
- Leave the work area clean and tidy for the next person
- Do not unplug or remove any IT equipment without the permission of a member of staff

Email

- Use St Hugh's e-mail for school and education-based purposes only
- Understand that e-mail messages are monitored
- Behave in a responsible way when using St Hugh's e-mail –are your communications true, helpful, necessary and kind?
- Report unwanted or inappropriate communications immediately

You are responsible for your behaviour and are accountable for your actions when using IT equipment, when connected to the St Hugh's network and when accessing the internet at school. Should you not keep to these rules, sanctions, in line with the School's Behaviour for Learning Policy, will apply.

Staff IT Acceptable Use Policy

The *Staff IT Acceptable Use Policy* outlines the rules for staff use of:

- internet access and St Hugh's email facilities
- computers, laptops and mobile devices provided by the school, in addition to any networking connecting them or peripheral hardware items
- laptops, smart phones, tablets and other personal mobile devices owned by members of staff when these are connected to the St Hugh's network via Wi-Fi.

Staff should note that these rules also apply to their personal devices when they are using a St Hugh's email account or app which enables access to documents and files from a St Hugh's Office365 account, even when they are not connected to the St Hugh's network.

Staff must observe the following points at all times and be aware that breach of this, abuse or inappropriate use of the network, internet facilities, hardware or software will result being subject to the School's *Disciplinary Procedure Policy*. Where the matter is considered to be serious or extreme, Police involvement may be necessary:

- The St Hugh's network and computer systems must be used only in connection with the duties for which the school employ staff members.
- The school acknowledges that limited personal use may occur from time to time. Any such use must be in accordance with this policy, and must not impede staff members' professional obligations.
- Hardware owned, leased, rented or otherwise brought onto the school site by staff may be connected directly to the St Hugh's wireless network which offers filtered internet access.
- Staff must not create, transmit or cause the transmission of:
    - material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence, or that is abusive, humiliating, hostile or intimidating.
    - offensive, obscene or indecent

      material o defamatory material
    - material such that the copyright of another person is infringed.
- Staff must not download files from unknown sources unless they have been scanned for viruses.

- No attempts to install unlicensed or personal software on any IT equipment belonging to the school - software installation must be agreed and carried out by a member of the IT department.
- Staff must not gain, or attempt to gain, deliberate, unauthorised access to any of the St Hugh's servers.
- Staff must not deliberately transmit any confidential information belonging to the school, or an individual's personal information by email, other than in the course of their formal duties and within the remit of their job descriptions.
- Staff must not gain unauthorised access to, or violate the privacy of, other people's files, corrupt or destroy other people's data or disrupt the work of other people.
- Staff must not disclose St Hugh's network passwords to third parties.
- Staff should familiarise themselves with the School's Data Protection Policies and their responsibilities for the protection of personal data.

Staff should follow St Hugh's School's E-Safety policy for staff and the Acceptable Use Policy at all times and have regard for St Hugh's School's E-Safety policy for pupils.

- Contact with pupils should be through St Hugh's authorised mechanisms i.e. school email addresses, home/school books
- Personal phone numbers, email addresses or communication routes via all social media platforms should not be used and staff should not share their home address with pupils or their parents. The exception to this would be if a member of staff has a child at the school and is contacting the parent re play dates etc. If contacted via an inappropriate route the member of staff must inform the Headmaster immediately
- Staff must not accept friend invitations or become friends with any pupil or parents/guardians of St Hugh's School on any social media platform unless they know them personally and not through their professional life
- Staff should also refrain from following the Twitter or other similar social media accounts of pupils or their parents.
- Staff must not engage in inappropriate use of social network sites which may bring themselves, the school or the school community into disrepute. Staff should adopt the highest security settings on any personal profiles they have.
- Staff should remain mindful of their digital footprint and exercise caution in all their use of social media or any other web-based presence they have. This includes written content, videos or photographs and views expressed either

directly or by ‘liking’ certain pages or posts or following certain individuals or groups. Staff should exercise care when using dating websites where staff could encounter students.

- Staff must not make contact with pupils, must not accept or initiate friend requests nor follow pupils’ or their guardians’ accounts on any social media platform. Staff must not communicate with pupils or their guardians via social media, websites, instant messenger accounts or text message. The only acceptable method of contact is via the use of school email accounts or telephone equipment.
- Staff should not make contact with pupils’ family members, accept or initiate friend requests or follow pupils’ family member’s account on any social media platform.
- Staff should not answer or use their phone or mobile device in lesson time unless it is in an emergency or if a member of SLT who is ‘on call’. Phones should be kept on silent at all times. This does not apply in EYFS where no mobile phones are permitted at any time.

Photographs

- Mobile phones and cameras which staff have on the school premises should not be used to take photographs of the children; with the exception of Twitter (see separate section) and on the rare occasions when no other device is available (see above).
- Only school cameras should ideally be used and then images or videos only downloaded onto school computers, so that their use can be monitored.
- Mobile phones are not permitted in the EYFS setting.
- Photographs of children may be taken on school equipment and may only stored on iSAMS or Earwig apps.
- Images and videos of St Hugh’s children should never be stored on personal devices.

Photography, video and images of children

- Many school activities involve recording images as part of the curriculum, extra school activities, publicity or to celebrate an achievement. In accordance with The Data Protection Act 1998 the image of a pupil is personal data. Therefore, it is a requirement under the Act for consent to be obtained from the parent/guardian of a pupil for any images made. It is also important to take into account the wishes of the pupil, remembering that some pupils do not wish to have their photograph taken or be filmed.
- Photographs/stills or video footage of pupils should only be taken using school equipment for purposes authorised by the school and should be stored securely

and only on school equipment. When a personal device has to be used (eg. When 'Earwig' is used for example) then staff should ensure no images are stored on their device.

- All photographs/stills and video footage should be available for scrutiny and staff should be able to justify all images/video footage made.
- Staff should remain aware of the potential for images of pupils to be misused to create indecent images of children and/or for grooming purposes. Therefore, careful consideration should be given to how activities which are being filmed or photographed are organised and undertaken. Particular care should be given when filming or photographing young or vulnerable pupils who may be unable to question how or why the activities are taking place. Staff should also be mindful that pupils who have been abused through the use of video or photography may feel threatened by its use in a teaching environment.

The school reserves the right to monitor staff communication and network storage in order to:

- establish the existence of facts
- ascertain compliance with regulatory or self-regulatory procedures
- monitor standards which are achieved by persons using the St Hugh's IT system in the course of their duties
- investigate or detect unauthorised use of the St Hugh's IT system
- gain access to routine business communications, for instance checking voicemail and email when staff are on holiday, sick leave or maternity leave.

Data
No data on children is to be stored on Office 365 but should be kept on ISAMs

Staff – Loan of School IT Devices Policy
Staff who use portable devices owned and maintained by St Hugh's must complete a Loan form accepting responsibility for its safekeeping. The terms of this loan are as follows:

- St Hugh's reserve the right to request the return of equipment at any time, and this will be actioned by you within 24 hours.
- In the event of your leaving the School's employment, you must return all St Hugh's IT equipment, including charging cables and other accessories, to the IT Department on or before your last working day.
- All staff will be installed on St Hugh's IT equipment as a limited user. When requests for paid applications and installations are sanctioned, this will be completed by the St Hugh's IT Department. For iPads, free apps may be downloaded by the user.
- It is expected that you will take care of School IT equipment as if it were your own, and that it will be returned in a reasonable condition, taking into consideration the age of the device and the length of the loan period.
- The use and care of the device remains a personal responsibility, which you should not delegate to a third party.
- Although School IT equipment is covered by the School's insurance policy, its value and the excess applied is unlikely to warrant the School making a claim in the case of damage or loss. It is therefore, the personal responsibility of staff to take due care and security precautions to protect the device at all times. If it is damaged or lost owing to your negligence, you could be asked to cover the cost of a replacement. You are advised to check your own personal insurance to determine whether you would be covered.

Staff responses to this loan agreement will be held by the Bursar

Useful resources for staff, pupils and parents

DfE advice for parents and carers on cyberbullying

DfE advice on use of social media for online radicalization

Keeping Children Safe in Education (September 2018)

www.nspcc.org.uk

www.getsafeonline.org

www.thinkyouknow.co.uk

www.kidsmart.org.uk

www.ceop.police.uk

www.saferinternet.org.uk

www.theparentzone.co.uk

www.bbc.co.uk/webwise

www.childnet.com

www.ThinkYouKnow.co.uk

www.disrespectnobody.co.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

www.educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation