ST. HUGH'S E-SAFETY POLICY

1. Introduction

1.1 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

1.2 Artificial Intelligence (AI), the internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

1.3 However, the use of these new technologies can put young people at risk within and outside the school. These risks can be categorised, but are not limited, to four types:

content: Harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories can be accessed by children and young people through a variety of technologies.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual) sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel that a child or young person in your care is at risk from this type of activity please report it to the Anti-Phishing Working Group APWG

1.4 Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies Policy review. This includes the Anti-Bullying

Policy and Positive Behaviour Policy as well as the Safeguarding and Child Protection policy. All of these are available on our website.

1.5 As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. At St Hugh's School Online Safety is taught directly in ICT and PSHE lessons, however the overarching principles of online safety are discussed and taught in every lesson where IT is used, this includes hobbies and clubs.

2. Scope Of The Policy

2.1 This policy applies to all members of the school community. This includes staff, pupils and parents of children in all age groups from 2 to 13 both as day pupils or in boarding.

2.2 Education and Inspections Act 2006 empowers Heads, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place in or out of school.

2.3 The school will deal with such incidents as they relate to this policy, the Positive Behaviour Policy or Anti-Bullying Policy. We will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place in or out of school.

2.4 This policy must be read in conjunction with Keeping children safe in education - GOV.UK (KCSIE) and further information is available here:

a. Teaching online safety in schools
b. Sharing nudes and semi-nudes: advice for education settings working with children and young people
c. Harmful online challenges and online hoaxes
d. Education for a Connected World
e. UKCIS Online Safety Audit Tool - UK Council for Internet Safety - GOV.UK
f. Safeguarding children and protecting professionals in early years settings: online safety considerations
g. Digital Resilience Framework
h. Online safety in schools and colleges: Questions from the Governing Board

3. Roles And Responsibilities - Communicated To Staff

3.1 The Head is responsible for:

- Ensuring the safety (including e-safety) of all members of the school community, the day to day responsibility for e-safety will be delegated to the DSL
- Ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role

3.2 ICT support is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That users may only access the school's networks through a properly enforced password protection policy
- The school's filtering system is applied and updated on a regular basis.
- That they keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

3.3 The Head of ICT is responsible for:

- Running e-safety training on a regular basis for staff and parents as well as ensuring it is embedded in the curriculum. This includes time at INSET meetings if necessary and information to parents
- An effective system for remote learning is in place when needed, following the school policy for remote learning

3.4 The Designated Safeguarding Lead is responsible for:

- Ensuring an effective e-safety curriculum is in place
- Liaising with the Headmaster about all safety matters
- Ensuring an effective filtering system is in place
- Monitoring the filtering and alerts generated
- Ensuring that all staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- Responding to any safeguarding issues flagged up by the automated filtering system
- Responding to any concerns raised by parents, pupils and staff

3.5 Teaching and Support Staff are responsible for ensuring that:

- They ensure no personal mobile internet enabled devices are used in school or on school transport and trips as per the Staff Code of Conduct.
- They report any suspected misuse or problem to the DSL
- Digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) will be on a professional level and only carried out using official school systems as per the Staff Code of Conduct.
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra curricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- They are aware of the risks of radicalisation, the Prevent Duty, indicators and influencers.

3.6 Boarding Staff will ensure that:

- Boarding policies and procedures are followed during all boarding activities, on site and off site.
- They follow the Staff Code of Conduct for internet use
- Children in their care are monitored when using school chromebooks, cameras or video equipment

3.7 Pupils will:

- Receive training and education about the four main areas of E-Safety: Content, Conduct, Contact and Commerce.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- If they are a boarder they have also been informed of the e-safety measures in the policies and procedures for boarding.
- Know and understand school policies on the taking / use of images, in particular that they must not take images or videos of other pupils unless it is part of a supervised lesson and they are directed to do so.
- Know and understand what cyber-bullying is and how to recognise and deal with any issues arising from it
- Understand how to raise concerns
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- Understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults.
- Know and understand how to use remote learning systems safely

4. Policy Statements - Education - Pupils

4.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of St Hugh's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

4.2 E-Safety education will be provided in the following ways:

- A planned e-safety programme is part of ICT and PSHE lessons and is regularly revisited – this covers both the use of ICT and new technologies in school and outside school including AI.
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. They are taught about misinformation, disinformation (including fake news) and conspiracy theories.
- Pupils will be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils will be taught what to do if they come across inappropriate material and who they can raise concerns with
- Staff will act as good role models in their use of ICT, the internet and mobile devices
- When working remotely, pupils must :
    - Be contactable during the school day in line with their timetable
    - Complete work to the deadline set by teachers
    - Seek help if they need it, from teachers or teaching assistants
    - Alert teachers if they're not able to complete work
    - Work in communal areas of the house

5. Policy Statements - Education – Parents/Carers

5.1 E-safety information for parents can be found on the school website. A copy of this policy is available for parents on the website. Internet Safety Updates are communicated to parents via email. Training for parents and further information is provided from CEOP, National Online Safety and the NSPCC.

5.2 Parents are also aware of the Remote Learning Policy. This will be sent to the parents again as and when remote learning is widely used.

5.3 Parents have been informed of the following:

- Devices such as e-readers may be used
- If pupils wish to use an e-reader they contact Mrs Natalie Wallis, Deputy Head (Pastoral) and Designated Safeguarding Lead.
- St Hugh's School is reliant on the support of parents at home in overseeing and managing any content downloaded on their child's device and in helping us to ensure that this is appropriate.
- Parents use appropriate filtering and monitoring for their children's devices to minimise any risks outside of school.

6. Policy Statements - Technical (Filtering and Monitoring)

6.1 The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- There will be regular reviews of the safety and security of school ICT systems.
- Servers must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.

- All users (from reception and above) will be provided with a username and password by the Head of ICT who will keep an up to date record of users and their usernames.
- The "master / administrator" passwords for the school ICT system, used by ICT Support Manager must also be available to the Headmaster and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the ICT Support Manager needing to switch off the filtering for any reason, or for any user, the Headmaster and DSL must be notified
- Ensuring the web filter is kept up to date and that reports are generated and checked for inappropriate sites by the DSL. Any safeguarding reports are automatically generated for the DSL.
- The filter comprises both user based filtering and a transparent proxy for other devices, managed by RM. Any visitors granted access to the school's wifi will have internet access filtered through the transparent proxy.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Pupil data cannot be transferred onto unencrypted devices or taken off site under any circumstances.

6.2 Parents will be responsible for the filtering and monitoring of personal devices outside of school. This includes access to personal devices and relevant checks.

7. Policy Statements - Curriculum

7.1 E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT across the curriculum using age appropriate resources

- In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines on the school system, staff must be vigilant in monitoring the content of the websites the young people visit.

- Students will be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students are helped to understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults.

7.2 Useful resources can be found at:

- Professionals Online Safety Helpline UK Safer Internet Centre
- Reporting Harmful Content Report Harmful Content | SWGfL
- CEOP
- Internet Watch Foundation. Internet Watch Foundation
- National Cyber Security Centre - National Cyber Security Centre

8. Policy Statements and Actions on the use of Digital and Video Images

8.1 Statements

- The development of digital imaging technologies, including AI, has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.
- However, staff, parents and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Furthermore with the development of AI and image manipulation individual pupils and whole schools may be at risk.
- At St Hugh's School we inform and educate users about these risks and implement policies to reduce the likelihood of the potential for harm. We review these policies as technology adapts and changes the risk to the pupils in our care.

8.2 Actions

1. Staff, volunteers and pupils are **not permitted** to use their own mobile phones, tablets or cameras to take or record any images of staff or pupils but instead must use the school cameras or tablets purchased or provided for the purpose. This applies to the whole school including those in the EYFS Early years foundation stage (EYFS) statutory framework - GOV.UK

2. We seek parental permission to take photographs of the pupils, this includes permission to use the images on the website or Class Dojo. Copyright notice: digital images, photographs and the internet - GOV.UK
3. Visitors to sporting fixtures, performances and plays are requested not to take pictures or videos of children other than their own unless they have a parents permission, and they are requested not to share images on social media.
4. When using digital images, staff inform and educate pupils about the risks associated with this, In particular they are encouraged to recognise the risks attached to putting images of themselves on the internet.
5. Pupils are instructed not to take, use, share, publish or distribute images of other people, including pupils and staff at St Hugh's School, without both their permission and the permission of the school even when using school devices.
6. Care will be taken when taking digital or video images using school devices that pupils are always appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
7. Photographs published on the website that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.Generative artificial intelligence (AI) in education - GOV.UK
8. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

9. Policy Statements - Data Protection

9.1 Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Only store any personal data in designated folders on the school network.
- Only transfer data using encryption and secure password protected devices.

10. Policy Statements - Communications

10.1 When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils therefore use only the school email service to communicate with others when in school, or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents and carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils will be provided with individual school email addresses for educational use.
- Pupils are be taught about email safety issues, such as the risks attached to the use of personal details. They are also taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information is not to be posted on the school website and only official email addresses are used to identify members of staff.

Pupil Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger" and will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping or file sharing
- I will not access video broadcasting sites (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will be polite and responsible when I communicate with others, respecting their views
- I will not take, distribute or publish images or videos of anyone without both their permission and the permission of the school.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will NOT use my personal hand held / external devices (mobile phones / USB devices etc) in school.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent it
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I will take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

When working remotely:

- I will only contact staff through the school's email system or Google Classroom
- Be contactable during the school day in line with their timetable
- Complete work to the deadline set by teachers
- Seek help if needed from teachers or teaching assistants

- Alert teachers if not able to complete work
- Work in communal areas of the house
- Be polite and courteous when messaging any member of the school community

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Signed:

Signature of Parent/Guardian:

Date:

Staff (and Volunteer) Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images under any circumstances. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has a responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use a personal device in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software
- I will not open any attachments to emails, unless the source is known and trusted
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, without prior agreement.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I will not store pupil personal data on any personal devices
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, termination of contract and in the event of illegal activities the involvement of the police.

Policy Last Reviewed	Autumn 2025
Policy Next Reviewed	Autumn 2026
Staff Responsible	DSL
Governor Review	
ISI Reference	n/a
Website	Yes