Hill House School Policy and Procedure

ICT – On Line Safety, including Acceptable Use Policy and Procedures

This On Line Safety Policy is part of our school's Safeguarding – Child Protection Procedures

Hill House School is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment. It is our aim that all students fulfil their potential.

Our approach to On Line Safety is directed and informed by *Keeping Children Safe in Education* (Sep 2023) and we recognise that online safety is part of the school's statutory safeguarding responsibilities.

The DSL has overall responsibility for online safety; and is supported by appropriately trained deputies.

All staff, across the school community contribute to safeguarding and as part of this the E-Safety Policy and the responsibilities are shared. Any technology used in school (regardless of ownership) shall be governed by this policy.

All staff (including governors) receive online safety information and training at induction. Online safety is addressed as part of whole staff regular child protection training

Networked computer resources and internet access are widely available at **Hill House School.** They enhance the learning environment for both teachers and students, but are sophisticated and powerful tools and internet use in particular raises a range of safeguarding, legal, ethical, technical and management issues. There is thus a need for proper regulation and guidance in the use of computers/devices and internet by staff and young people. All those who wish to use the system must comply with the policy.

The students are given supervised access to our computing facilities/devices and will be provided with access to monitored and appropriately filtered internet and other services operating at **Hill House School.**

The students are taught about online safety as part of statutory Relationships and Sex Education and PSHE, this curriculum is tailored to meet the needs and understanding of our students

The school recognises that child-on-child abuse, including sexual violence and sexual harassment can occur online. All staff have an essential role to play in both preventing online child-on-child abuse and responding to any concerns when they occur, even if they take place offsite and should have

The risks for our students;

Content risks
For school-age children these risks include things that they might find upsetting, disgusting or otherwise uncomfortable, if they come across them accidentally. This might include sexual content in games, pornography, images of cruelty to animals, and real or simulated violence.

Contact risks
These risks include children coming into contact with people they don't know or with adults posing as children online. For example, a child might be persuaded to share personal information with strangers, provide contact details after clicking on pop-up messages, or meet in person with someone they've met online.

Conduct risks
These risks include children acting in ways that might hurt others, or being the victim of this kind of behaviour. For example, a child might destroy a game that a friend or sibling has created. Another conduct risk is accidentally making in-app purchases.

Commerce risks
These risks include children signing up to unfair contracts, terms or conditions that they aren't aware of or don't understand. For example, children might click a button that allows a business to send them inappropriate marketing messages or collect their personal or family data. Or children might use a toy, app or device with weak internet security, which leaves them open to identity theft or fraud. It includes risks such as online gambling, inappropriate advertising, phishing and or financial scams.

How will students keep safe and learn to evaluate Internet content?

- If staff or students discover unsuitable sites, The URL (address) and content must be reported to the ICT technician.
- Staff and students should ensure that their use of Internet derived materials complies with copyright law
- Students should be taught to be aware of the materials they read and some awareness of the risks of going online.
- All students and young people's devices are protected by the Kaspersky monitoring and filtering Application and reports of misuse are recorded and sent to the E-Safety lead and ICT Technician
- In accordance with `*Keeping Children Safe In Education`(2023)* – The Monitoring and filtering is in place at Hill House School and student/staff usage is regularly reviewed to ensure the effectiveness of the monitoring and filtering system

- When and where appropriate students will be taught to acknowledge the source of information used and to respect copyright
- All students have an Individual risk assessment for on line safety and this is reviewed regularly.

Access to Computers:

- Access to the school network is available from any network station during the normal school day in lesson time **with an adult supervising**. Computer/device access is available during care time and school holidays **under close adult supervision.**
- A risk assessment is carried out for each student outlining their access and ability to use ICT and advice given to staff on the level of supervision before use in school is allowed.
- The unauthorised access or use of personal information, contrary to the previsions of the Data Protection Act is not permitted.
- School ICT systems admin and the SMT will ensure that ICT security systems will be reviewed regularly.
- Virus protection will be updated regularly.
- If a 'virus alert' occurs when transferring work from one mode to another the IT technician should be informed immediately. All external hardware e.g. the use of Memory sticks should be avoided but if their use is essential must be vetted by submitting them to an anti-virus check.

E-mail Usage:

- Staff must not reply if they receive an offensive e-mail and must **immediately inform a member of SMT.**
- Students must not reveal details of themselves or others in e-mail communication or via a personal web space, such as their age, the location of the school, messaging account details, an address or telephone number, or arrange to meet anyone. **Adults supervising the students whilst they are using ICT must make the SMT aware of inappropriate use or online communication between students and the outside world.**
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

Published content and the school website:

- Staff or students personal contact information will not be published on the school website. The only contacts details given on our website will be the school address and telephone number.
- Students full names will not be used anywhere on the school website or other on-line space.

- We will use photographs of children's work when communicating with Parents/guardians and the wider community, in newsletters and in the school prospectus.
- Photographs will be checked to ensure that they are suitable (photos of children in swimwear would be unsuitable).
- Photographs used will not be captioned with children's names.

Staff Use of mobile devices and technologies:

- The use of mobile phones by staff - when on site, mobile technologies **should only be accessed in the staff room during break time** - unless with prior written approval of the Principal. Mobile phones should be left in the staff room or in staff vehicles and should not be kept upon your person whilst on duty.

Social networking:

- **All staff at Hill House have an overriding responsibility to act and to conduct themselves at all times in a manner which makes a positive and active contribution to the education and welfare of the children in our school and in our care** - *Hill House Staff Code of Conduct*

Social networking sites

Staff must not have any images of, school students or parents on their personal pages on social networking sites. Staff must not accept students and young people or parents as "friends" or "contacts" on these sites and must ensure the highest privacy controls are used at all times on their personal pages on such sites. **Failure to do so is a disciplinary matter**. Inappropriate adult behaviour which must be avoided also includes:

- Talking inappropriately about sex lives particularly in front of students
- Being alone with students in a group setting for unusually long periods of time without good reason
- Showing unusual interest in one specific student
- Use of personal devices where messages, browsing, calls or texts take attention away from supervising students.

It will be best practice if:

- Staff should not access social networking pages on school computers, tablets or mobile devices. The school will not allow access to social networking sites such as Instagram, Snapchat, Facebook or Twitter for students or staff.
- Students will be advised never to give out their personal details of any kind which may identify them, their friends or their location.
- Students and Parents/guardians will be advised via our safeguarding newsletters that the use of social network spaces outside school brings a range of dangers for our students.

- Personal mobile phones should be left in the staffroom or in your car and **NOT** carried with you throughout the day. Phones should only be used in the staffroom during breaks and not in any other location
- If you have any social media account e.g. Facebook, please remember this is for your personal use only. **You must not have any images or references to the students in our care, yourselves at work, your colleagues or Hill House and The Cambian Group**
- We must respect our student's dignity and keep them safe!
- We all have a responsibility to report anything that we see that we are uncomfortable with
- It is important for you to think through the possible implications of using social media as failure to keep to the required standards could be a disciplinary matter
- Always remember that you are personally accountable for what you say and do on-line

Authorising Internet Access:

- All staff must read and sign to say they have read the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- Staff have a duty to be aware of the students IRAs for the use of ICT before allowing a student access to the ICT resources.
- We will maintain a current record of all staff and students who are granted access to school ICT systems.
- During education time access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents/guardians will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.
- **Students and staff should understand that Internet use will be monitored**
- All new staff will be taken through the key parts of this policy as part of their induction
- All staff including teachers, learning support assistants and support staff will be provided with the School On Line Safety Policy and have its importance explained as part of the safeguarding and child protection training requirement.
- Staff will be informed that network and internet traffic can be monitored and traced to the individual user.
- Staff development in safe and responsible internet use, and on the school Internet policy will be provided as required
- Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.
- Staff will read and sign *Staff Code of Conduct for ICT*- prior to using school ICT equipment in the school

Acceptable use by Parents/guardians and carers

- Partnership working with Parents/guardians and carers should be considered essential practice for promoting an agreed and consistent message which will define acceptable

and unacceptable behaviour. Should Parents/guardians or carers wish to use personal technologies, such as cameras within the setting environment, authorisation must be obtained from the Senior Designated Person for Safeguarding. Specific guidelines for the use of such technologies must be followed

- In accordance with `*Keeping Children Safe In Education`2023* where the students are accessing remote learning – We communicate with parents about the importance of children being safe online, what systems we have in use at school and will make parents/carers aware of what we are asking them to access and being clear about who from the school (if anyone) the child may be interacting with online

Acceptable use by Governors, visitors, contractors and others

- All governors receive appropriate online safety information/training as part of their safeguarding and child protection training; this is received as part of their induction and is regularly updated.

- Governors ensure that the school leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

- All individuals are to be expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with children and young people. All guidelines in respect of acceptable use of technologies must be adhered to. The right to ask any individual to leave at any time is to be reserved.

- Visitors to the site may not use mobile devices without prior authorisation from the SMT.

The following will apply to all:

- Do not use ICT without permission.
- Food and drink must not be consumed near any computer equipment/devices anywhere in the school.
- Do not move about the room while seated on a chair.
- Any person found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement.
- Computer faults should be promptly reported to the ICT Co-ordinator. Please do not attempt to repair them yourself.
- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at the workstation.
- Mobile phones should not be used in school work time unless for stated school purposes and agreed with the SMT

- **Staff should not allow students to use computers or devices that are running on the staff members login**

At the end of a session:

- Log off/shut down according to instructions.
- Replace laptops as directed.
- Treat ICT equipment with respect and keep areas around ICT equipment clean and tidy.
- Normal school rules and consideration of others applies.
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

Security and Software Licensing:

Security is especially important in schools, where vigilance is needed at all times to be ready to detect any forms of personal intimidation and exposure to inappropriate material. It is therefore very important that users' accounts are used only by themselves; otherwise they are exposed to impersonation by another user. Where education and care staff have access to a student's account this must have been agreed to by a member of the SMT and form part of their "best interests" protocols.
The following rules are industry standard:

- Always log out of your computer when you have finished, or if you have to leave it unattended.
- Do not let anyone else log in to a computer using your username and password.
- Do not tell anyone your password; you are responsible for keeping it secure.
- **Staff are not permitted to install software or programs onto computers without the prior authorisation of the ICT technician.**

Monitoring and Filtering:

All devices are protected by Kaspersky and monitoring and filtering is individually set up for each student dependent on their level of risk

Safe search blocks the student from being able to access inappropriate content from search results on Bing, Google and Yahoo. Kaspersky safe kids additionally blocks the following website categories from appearing in search results; Adult content, Alcohol, tobacco, narcotics, Profanity, obscenity, extremism, racism

The following is also in place;

- A review of student needs regarding monitoring and filtering is undertaken annually as part of the review of the Online Safety Individual Risk Assessment - or as when necessary and requested as need/concerns arise
- All incidents of monitoring alerts are kept and a record of follow ups is included. This record is updated weekly

- The IT Lead follows up requests for further information
- This report informs the Individual Risk Assessments and safeguarding training for staff
- Hill House has a Local Online safety and Acceptable use policy which is reviewed annually
- The IT Lead renews licences and manages the Kaspersky APP ensuring that all new devices are protected both in the home and in school/college
- The IT Lead keeps a record of onboarding and off boarding devices
- The IT lead ensures that all devices are kept in good order and that all necessary safeguarding, monitoring and filtering protections are activated

Security on the Internet

- Do not type any personal details (including your name or email address) into a web site unless you are absolutely sure of the authenticity and trustworthiness of the associated company.
- The use of chat rooms is prohibited.
- The use of Instant Messaging is prohibited.
- The use of Internet-based email or newsgroups is prohibited except with the prior written approval of the Principal.

Downloading Material from the Internet:

- Do not download or copy any material from the Internet unless you are sure that the source is reliable and that there are no copyright, intellectual property right or licensing restrictions. If in doubt, ask the ICT Technician.

Key Messages

Safeguarding and On Line Safety

- The On Line Safety Individual Risk Assessments are regularly updated and can be found in their master care files.
- These are important documents – it is part of our **duty of care** to the students to monitor and protect our students from accessing inappropriate material on the internet both in their home and in education.
- It is key that you support the students with their use of ICT and if you feel that they have been exposed to something harmful, to talk about this with the student if appropriate, and to **report** it to the SMT.
- It may not always appear immediately obvious to us if a piece of video, music etc. is harmful, it may at first glance seem flippant and humorous, however we need to

be very alert to the possible impact or messages that may be given via the internet to our students.
- We must not let our students have unguided access to You tube and its equivalents.
- We do have a filtering system in place but it is not 100% failsafe and even so, what may appear as harmless content can still have an impact upon our students' attitudes and presenting behaviours.

Monitoring and Review

- This policy will be subject to continuous monitoring, refinement and audit by the Principal.

Principal of Hill House;
Kate Landells
Hill House School, Boldre, Lymington, Hants. SO41 8NE
Tel: 01590 672147
Email:

September 2023

Review Date September 2024