HARRODIAN

Online Safety, Internet use and computer, laptop and mobile device use at The Harrodian School

ICT Policy

Introduction

The Harrodian School recognises that the use of Information and Communication Technology (ICT) is essential to modern life and an integral part of the school's modus operandi. However, we also recognise that technology brings with it potential dangers. Indeed, as the technology evolves, so too do the dangers. No school can foresee future developments, and so an ICT policy inevitably will be reactionary. It is our intention, within that caveat, to be as up-to-date as possible.

Our Policy has been written by the School, building on a National Grid for Learning (NGfL) policy template and the Ofsted document "Inspecting e-safety". This document should be read in conjunction with the School's policies on behaviour, safeguarding, anti-bullying and data protection. It will be reviewed annually. Changes will be made immediately if technological or other developments so require.

This Policy should be made available to all via the main school website. Other information including online safety tips for staff, pupils and parents will also be posted on the school website.

Roles and Responsibilities

Role	Key Responsibilities
Deputy Head & Safeguarding Lead	• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security ensuring that the school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including a filtered Internet service • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

Role	Key Responsibilities
	• To be aware of procedures to be followed in the event of a serious online safety incident • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure the school website includes relevant information
Online Safety Co-ordinator and Head of Computing	• **Coordinate curriculum input** • Liaise with other teachers in the department (Lucy Horan, Toby Huelin and one other to be confirmed) to cover e-safety in a progressive way. PP2, PP3, 8s, 9s, 10s, 11s & 13s at the beginning of year. • **Coordinate extra-curricular training for pupils** • Prep seminar: visiting speakers in conjunction with Head of Lower Prep • Anti-bullying week: 13-17 November 2017 • January 2017: Police talk to 12s & 13s: "Cyberbullying" • January: Digital Awareness UK talk in the Theatre: 10s, 11s, 13s, 14s, 15s. • Intel Security talk to 8s • 13s PSHE session after summer exams • **Coordinate training for parents** • Peter Cowley from Achieving for Children to speak to all parents • Prep parents' coffee morning and Online Safety presentation • Pre-prep parents' seminar in PP3 classroom • **Arrange staff training** • Beginning of the year. Prepare material or organise external speaker. Publicize latest news, best practice, e-safety incident procedure & incident log. • **Coordinate Safer Internet Day** • Present to Prep School in assembly (Tues 6 February 2018) • **Write, amend and publish Online Safety Documents** • Review Online Safety Policy (ongoing... write-up changes over summer) • Review staff handbook entry before Easter. • Review pupil planner entry before Easter (Prep, Senior and Sixth form). • Update official documents and resources on Harrodian.com website. • **Chair Online Safety Group** • Meetings (est: 4 per year). (Members: Heather Locke; Kris Kreis; Alison Heller; Andy Woodward; Peter Hardie; Jenny O'Neill; Ben Roets; David Behan; Rob Stewart; Lucy Horan) • Review Online Safety Incident Log

Role	Key Responsibilities
	• Discuss policy • Coordinate upcoming initiatives • Liaise with student council • **Monitoring and sharing information** • Attend relevant CPD courses (e.g. CEOP). • Research, stay up-to-date and share information in the news, via Twitter hashtags, Google alerts, email lists, youtube subscriptions, etc. • Monitor [anonymous] reports sent via SWGFL Whisper button on school website. • Monitor references to "Harrodian" and other keywords via Mention service. • Update information on jgledhill.co.uk with news feeds, information & resources for staff, pupils & parents. • Continue with 360degree safe review. • To undertake any other reasonable related tasks as requested by the Headmaster, Deputy Headmistress or Senior Management Team.
Network Manager	• To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • To keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • To regularly monitor the use of school technology and online platforms and report any misuse/attempted misuse to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Data and Information Managers	• To ensure that the data they manage is accurate and up-to-date • To ensure best practice in information management i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • To ensure the School is registered with the Information Commissioner
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)

Role	Key Responsibilities
	• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff ICT Use Policy, and understand any updates annually • To report any suspected misuse or problem to the online safety coordinator • To model safe, responsible and professional behaviours in their own use of technology
Pupils	• To read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school • To contribute to any surveys that gather information about their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • to consult with the school if they have any concerns about their children's use of technology

School computers, the School network and monitoring

The School has a networked computer system, which provides, amongst other things, Internet access to pupils and staff. This policy will help protect pupils, staff and the school by clearly stating what is acceptable and what is not. The school may exercise its right, by electronic means, to monitor the use of the school's computer systems, including the monitoring of web sites visited and emails sent: the school's IT Network Manager will coordinate this.

Acceptable Use Policies (AUP)

"Acceptable use" of the School computers and the School network is detailed here, and is also summarised in the following places to ensure easy reference:

- The AUP for staff is provided in the Staff Handbook, a document which must be read by all staff at Harrodian (this is a contractual obligation).
- The AUP for pupils is provided in the Pupil Handbook, a document which must be read by all pupils at Harrodian (it is the role of the Form Teacher to enforce this).

The purpose of the Acceptable Use Policies is to clarify that:

- Access must only be made via the user's authorised account and password, which must not be given to any other person.

- School computer and Internet use must be appropriate to the pupil's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the School or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.

Internet access for pupils

We offer pupils supervised access to the Internet.

- Within lessons, staff will guide pupils towards appropriate materials, however senior pupils also may have access to the Internet outside of lesson time.
- Pupils from Reception to Year 8 (12s) must always be supervised by a member of staff.
- Year 9s (13s) and above can access the Internet independently, but must understand that they may be monitored remotely.
- Note: whilst our aim for Internet use is to further educational goals, there is a possibility that pupils may possibly access other material, which could be illegal, defamatory, inaccurate or potentially offensive to some people. We do operate a filtering policy and will instil in pupils the need to be self-regulating in addition to this (with sanctions if they fail to be so).

Internet content and filtering

The school employs an industry standard content filter, (London Grid for Learning), which is regularly updated with blacklists, banned sites and banned phrases. Filtering is reviewed on an on-going basis.

- The person in charge of making regular checks to ensure that the filtering methods are appropriate, effective and reasonable is the IT Manager.
- Staff will report any inappropriate material found on the Internet that appears not to be filtered effectively.
- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users can only access appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- Prevent Duty: content filters and monitoring aim to ensure that pupils are safe from terrorist and extremist material when they access the Internet.

Online Safety education

The school does not attempt to “lock down” access to the Internet, but rather to manage and filter the services provided to an appropriate degree. The school also understands that it is possible that pupils and staff could access the Internet using methods that cannot be managed or filtered by them e.g by using cellular data (for example a 4G connection via a mobile phone). The school

believes that it is vital to educate pupils, staff and parents as to the possible risks that may be encountered online, and what to do if there is a problem. This is addressed in the following ways:

- Pupils are taught about Online Safety in Computing lessons, typically at the beginning of the school year.
- Pupils answer a questionnaire to assess their knowledge and understanding to help inform teaching and learning requirements.
- Peer mentors, e.g. Senior Prefects are used where possible, particularly in response to an incident.
- Opportunities are taken to speak to parents at parents' evenings.
- Staff are taught about Online Safety at least once a year, typically in an INSET environment.
- Parents are offered seminars at least once a year.
- Parents are offered information via the school website, and they are sent letters and other correspondence as situations arise.
- There is a focus on Online Safety at various times in the year, notably Safer Internet Day in February.
- The Online Safety Coordinator regularly updates a website: www.jgledhill.co.uk with information, resources, news and advice, for pupils, staff and parents. The Online Safety Plan for the year is included on this website.

Online Safety Group

A "Group", chaired by the Online Safety Coordinator, and including Section Heads, the IT Manager and Safeguarding leads meets at least once a term to discuss the following:

- Any incidents recorded via the Online Safety Incident Log and action that may be necessary following them.
- Any amendments to the ICT Policy that may be required.
- Any upcoming initiatives that can be used to promote Online Safety throughout the school community.

Email

The Harrodian School provides email accounts to staff and pupils as an official communication tool. The email system is intended to enhance communication between staff and pupils, but it does not replace the natural, direct communication in person that occurs during daily interaction. In order to ensure effective communication, users should log in to their email accounts *at least once every 24 hours*. Users are responsible for email they send, so emails should be written carefully and politely. As messages may be forwarded, email is best regarded as public property. All email users must abide by the guidelines set out below.

Purpose and use

The following are some of the ways in which email may be used. This is not intended as a comprehensive list. Pupils should be aware that different members of staff may establish their own arrangements for use of the email system within a given subject.

By staff:

- Communication by the school of important information.
- Reminders about term dates, academic deadlines and special events (for example talks, meetings and assemblies).
- Updates about sports fixtures, squads and training times.
- Reminders about work to be completed and/or instructions on work missed (at discretion of individual staff).
- Notification of detentions or other matters concerning a particular pupil.
- Other forms of communication as directed by the teacher.

By pupils:

- Communication between pupils related to schoolwork.
- Sharing of work between pupils involved in collaborative projects.
- As directed by teachers: communication with external parties for the purpose of research activity related to schoolwork.
- Pupils contacting teachers to request work missed due to absence.
- Other forms of communication as directed by teachers.

Email Quotas

The email quota is the amount of email (including attachments) that can be stored on the central email server. If a pupil's assigned allocation is filled up, no new mail can be received. As such, it is important to download attachments and remove them from the email inbox. Frequently, the size of an attachment is the factor that puts a mailbox over quota. The maximum size of any email attachment is 2MB.

Inappropriate use of email

The following activities are unacceptable when using email, or indeed other forms of communication such as social media (see also the section on "Use of social media"):

- Online Bullying (also known as cyberbullying) in any form.
- Using, transmitting or receiving inappropriate, offensive, vulgar or obscene language or materials.
- Making threats or insults.
- Sending unsolicited and unauthorised mass email (spam), or anonymous messages or chain letters.
- Using threatening or insulting language towards or about another individual.
- Making racist, sexist or homophobic jokes or jokes at the expense of people with disabilities.
- Infringing upon other people's privacy.
- Using another pupil's account to send information purporting to come from that person.
- Uploading a virus, or harmful, corrupted data.
- Misrepresenting or making disparaging comments about the Harrodian School.
- Using email to receive, forward or reply to messages intended to offend, embarrass or otherwise undermine pupil morale.

- Unless authorised to do so by a member of staff, pupils are forbidden from using email to communicate confidential information, for example any information about the Harrodian School, its pupils or its staff, to outside parties.
- Pupils may NOT use email to inform the Sports staff of non-attendance at training or fixtures. Such communication must take place in person.

Restriction

Access to and use of pupil email is a privilege accorded at the discretion of The Harrodian School. The School maintains the right to withdraw the access and use of pupil email when there is reason to believe that unacceptable activities have taken place. The pupils involved in such activities will be disciplined appropriately; such discipline may ultimately include expulsion from the school.

Staff and pupils should be aware that email accounts and Internet traffic can be monitored by the school and traced to the individual user.

Social Media

Current and emerging web technologies, such as instant messaging, blogs, chat rooms and video and photo sharing applications, increasingly allow interaction between users who can "post", "comment", "share", "Tweet", "like", "pin", "friend", "unfriend", and so on. Such sites are known as "social media" or "social networks". Teachers, pupils, exam boards and software suppliers to the school increasingly want to harness these features for teaching, learning, organisation, collaboration, creation of resources, sharing information and curating educational content. If these services are used to deliberately upset someone it is called "Online Bullying" (previously known as "cyberbullying"). Online Bullying is not tolerated by the school and is acted upon in accordance with the school's Anti-bullying Policy. Many of the same principles and rules apply as can be found in the section "**Inappropriate use of email".** The following rules and guidelines cover interaction between staff and pupils using such technologies:

Email and Moodle

- For 2-way interaction, staff should use the following approved and monitored methods of communication:
    - The **school email** system (www.harrodianschool.com/webmail). For more information see the section on Email.
    - The Harrodian School **Moodle** site.

Twitter

- Staff can post in public to a **Twitter** feed, to facilitate their role, improve communication or enable them to fulfil exam board requirements.
    - The utmost care should be taken to ensure that this does not expose pupils to any information that does not pass the "school noticeboard" test (in other words: would the content be suitable for pinning on the school noticeboard?)
    - Staff should not initiate or accept "private" interactions.

Google

- Staff may use **Google+** to facilitate their role, improve communication or enable them to fulfil exam board requirements, with the following provisos:
    - A member of the IT support team should double check privacy settings – this check should be confirmed in writing (email suffices here).
- Staff may use **YouTube** (a Google site) to host videos relevant to school work, sport, extra-curricular work, drama, or other valid purpose.
    - Content featuring pupils should be *private* and not publically viewable or searchable.
    - Current pupils may have a link to the video as required.
    - Staff should ensure that there are no pupils featured from the "no photos" list.
- Staff may use **Google Docs** to share, and collaborate on, documents, spreadsheets, presentations and forms.
- Care should be taken when using **Google Drive**, or indeed any cloud-based storage facility, at school. Staff should not backup large quantities of data (e.g. music, photos or video) as this steals bandwidth from valid school uses.

Other

- **Texting** a pupil (e.g. using *SMS, MMS, Whatsapp, Kik,* etc**.**) or calling their mobile phone should be avoided, unless, for sixth form pupils only, it is used for urgent school business, such as the sixth former being late for a school trip meet up.
- **Blogs** may be needed for valid curriculum purposes (e.g. Media Studies) and should be agreed with the IT Network Manager for security purposes. Use of blogs should, thereafter, be monitored carefully as it is possible that inappropriate content can be accessed this way.
- Currently there are instances of staff using a **pupil's personal email address**. We are in a period of transition to a fully adopted school email system with a comprehensively populated address book. If requested to by the pupil, to facilitate matters relating directly to the school (e.g. yearbook entries), staff may reply to such emails until further notice.
- No use of **Facebook** for pupil contact.
- Note also: particular care should be taken when using social media to communicate with **ex-pupils**, especially if they have recently left the school and include current pupils in their networks.

Conclusion

Use good judgement. Regardless of privacy settings, assume that all information shared online is public information. All communication traceable to the school should be related to school business and should be framed in the same professional manner as a formal letter or noticeboard post. Care should be taken by staff to keep personal information private. Staff should seek to correct any mistakes immediately, advising senior management of "major" mistakes such as a breach of security or confidentiality. Any breaches of the ICT Policy may lead to disciplinary action.

Mobile Telephones and Digital Photography

The School recognises the usefulness of mobile telephones (a term which is intended here to include smartphones, tablets and other portable electronic devices) as an effective means of communication, organisation and as an added personal security measure.

- Mobile telephones may not be used on the school site unless under the direct supervision of a member of staff. Pupil mobile phones will be confiscated if they are used during the working day.
- The use of any device to take photographs or video recordings is banned unless supervised by a member of staff for a legitimate school purpose.
- Staff should be careful not to have photographs of pupils on personal devices: rather use the school camera to take photographs for school publications, storing photos on secure network drives.
- Care should be taken to adhere to the "no photographs list" of pupils who do not give permission for photographs of them to be used (even for valid school uses such as school magazines).
- Parents and visitors may wish to take photos or videos, of school productions for example. Footage taken in school should not be uploaded to any social media sites. If students on the "no photos list" appear in a particular production, then clear instructions should be given before the event that no footage may be captured.

The use of laptops in lessons

The Harrodian School recognises that the use of a laptop in the classroom, for homework and for exams, is an important element of support for pupils with specific learning needs. This usage is carefully monitored by the Learning Support Department to ensure that the specific needs of each pupil are met. It is not seen as a total replacement for handwritten work, but rather as a means of allowing pupils the best possible means of expressing themselves on paper.

Identifying pupils as laptop users

Pupils are identified as potential laptop users by teachers, parents and staff. The main criteria for identification are:

- Poor, slow, illegible handwriting, where it is apparent that fluency is lost because of the effort involved in concentrating on the mechanical aspect of handwriting.
- Slow and/or inaccurate copying from the board, where weak visual processing makes it difficult for a pupil to move his/her eyes from paper to board and back.
- Messy presentation, which makes written work a problem for the pupil to refer back to and difficult for teachers to mark.

Once a pupil has been identified, it is the responsibility of the Learning Support Department to assess the pupil's eligibility to use a laptop. This assessment is done by making close comparisons between timed writing and typing, and by ensuring that the pupil has the necessary word-processing skills to manage a laptop efficiently.

It is essential that any pupil wishing to use a laptop in class can touch-type at a speed that matches and preferably exceeds his/her handwriting speed. He/she should also be proficient in word processing, using editing short cuts and saving and accessing files efficiently.

Only when these requirements have been met may a pupil begin to use a laptop as his/her preferred means of writing. He/she will be asked to sign a contract agreeing to use the laptop sensibly and appropriately and to take full responsibility for it.

Laptop use guidelines

The use of laptops in lessons will be at the discretion of the teacher and only for those pupils who have permission to use laptops in examinations. This requirement has the virtue of not prohibiting laptops for those pupils who are genuinely using them for note taking or other classroom activities.

Requests for pupils to use laptops in lessons or examinations must be initiated by teachers, not pupils. The Learning Support department will then ascertain whether the normal or efficient working of a pupil would be enhanced if they used a laptop and that it was their usual working method.

Pupil agreement:

I understand that using a laptop in lessons is a privilege and that failure to follow the guidelines listed below will result in this privilege being withdrawn for a period of time by my teacher.

I must take responsibility for my laptop, bring my charger and USB memory stick to school and ensure that everything is securely stored in my locker when not in use.

During lessons, I will:

- *Keep my laptop closed (screen down to keyboard) until my teacher informs me that I can use it.*
- *Only have those programs open that are required for the lesson.*
- *Not attempt to use the Internet during lessons unless my teacher gives me permission to do so.*
- *Not attempt to use spelling or grammar checking devices unless given permission to do so by my teacher.*
- *Not allow the use of my laptop to become a distraction to other pupils in the lesson.*
- *Keep safety in mind and ensure that if I need to plug in my laptop to a wall socket the wires do not trail and cause a tripping hazard.*
- *Ensure that all my work is saved securely on my hard drive and/or USB memory stick.*
- *Print off all homework and classwork before I come to the lesson.*
- *Print off any notes made in class as required by my teacher.*
- *File or stick into my exercise book all printed notes, classwork and homework.*
- *Remember that my laptop is not a replacement for other equipment needed for my lesson; I must also bring my textbook, exercise book or file and pencil case.*

Use of laptops in public examinations
Special arrangements are made for pupils to use a laptop in public examinations, according to the JCQ Guidelines. This is coordinated by the Learning Support Department.

Lower down the school laptops are permitted for exams at the discretion of the Learning Support Department and Form Teacher.

The Harrodian School website and official publications

Website and magazine photographs, that include pupils, will be selected carefully and will not enable individual pupils to be identified: pupils' full names will not be associated with photographs. Pupil photographs will immediately be removed from publications upon request from parents, or other appropriate request.

Data Protection

The School is required to process the personal data of pupils, their parents and guardians as part of its operation. Examples of personal data are: names and addresses; academic, disciplinary, admissions and attendance records; references; examination scripts and results. It shall take all reasonable steps to ensure the security of personal data in accordance with this Policy and the Data Protection Act 1998 ("the DPA").

Staff must:

- Only access personal data relating to pupils and parents/guardians where it is necessary for them to do so.
- If possible, access personal data relating to pupils and parents/guardians while on-site. When it is necessary to access data while off-site, staff must ensure that the data is secure (i.e. log off the system when not in use and ensure personal data cannot be seen by any other person).
- Gain permission from the Deputy Head prior to printing or copying any pupil or parent data.

What to do with concerns and incidents

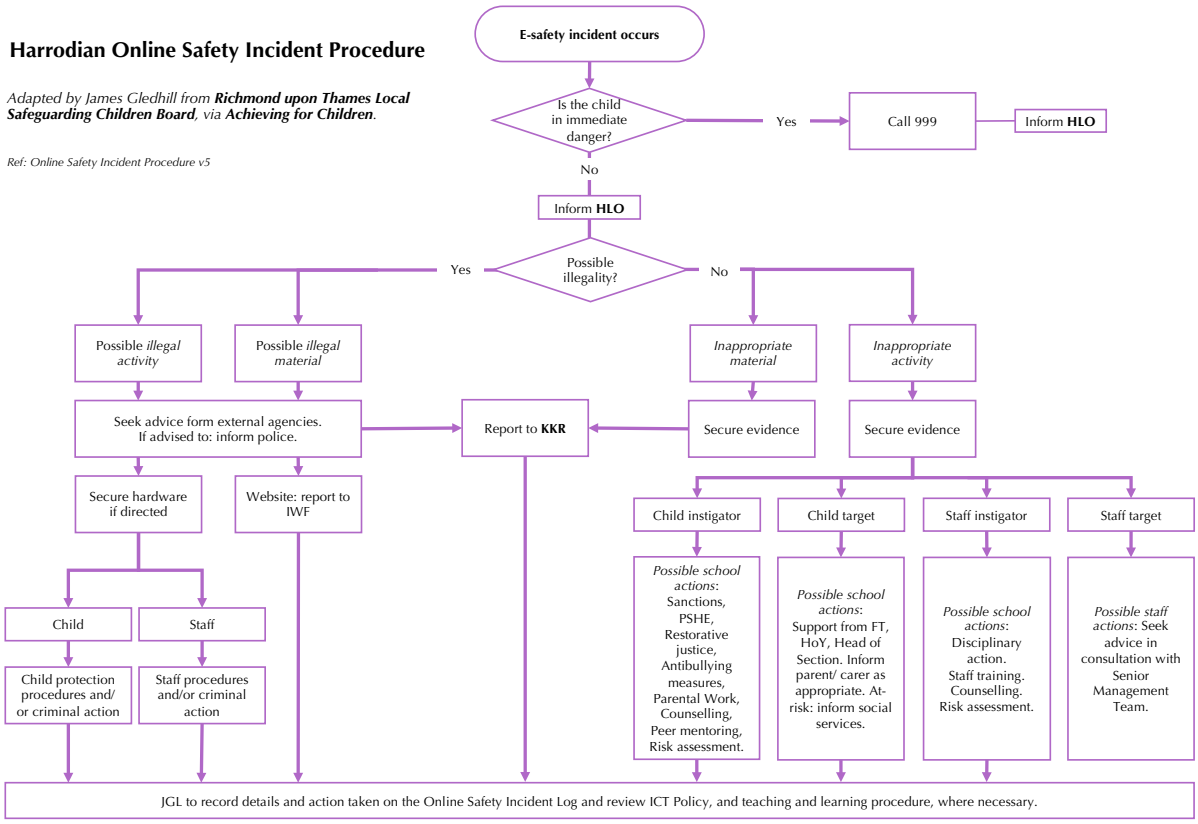
If you are made aware of an Online Safety incident, please inform Heather Locke in the first instance (with the caveat that if a child is in immediate danger, then the police should be called on 999). From that point the procedure should follow the flow chart included below. Note:

- **Do not delete** any images, chat threads, etc. as they may be needed as evidence.
- **Do not forward** any images, chat threads, etc. as it may not be suitable to distribute inappropriate or concerning material.
- For general help and advice, the national crime agency "**CEOP**" is a useful first port of call for all concerns: https://www.ceop.police.uk/Safety-Centre (also linked from the Harrodian School Website).
- Online Safety concerns may be reported anonymously to the Online Safety Coordinator via the SWGfL Whisper ***"Report an Issue"*** button on the Harrodian school webpage.

Harrodian Online Safety Incident Procedure

Adapted by James Gledhill from ***Richmond upon Thames Local Safeguarding Children Board****, via* ***Achieving for Children****.*

Ref: Online Safety Incident Procedure v5



Person responsible: Mr J Gledhill

Last update: September 2017

Next update: September 2018