HARRODIAN

Online Safety Policy

Introduction

Harrodian 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 Online Safety 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 at least annually. Changes will be made immediately if technological or other developments so require.

This Policy is 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 and 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 • To be aware of procedures to be followed in the event of a serious online safety incident

Role	Key Responsibilities
	• 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 David Redhead) to cover e-safety in a progressive way. PP2, PP3, 8s, 9s, 10s, 11s and 13s at beginning of year. • **Coordinate extra-curricular training for pupils** • Prep seminar: visiting speakers in conjunction with Head of Lower Prep • Anti-bullying week: Mid-November • January: Police talk to 12s and 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 and incident log. • **Coordinate Safer Internet Day** • Present to Prep School in assembly. • **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)

Role	Key Responsibilities
	• 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 • 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 and resources for staff, pupils and 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 • That they 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

Role	Key Responsibilities
	• That the use of School technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported 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 • 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 • The School must be registered with the Information Commissioner
Website managers	• To ensure safeguarding of any children appearing on our public website by omitting surnames and any details • Strictly adhering to the 'no photos' list of children • To ensure that @HarrodianNews twitter account is monitored regularly to avoid any misuse
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) • 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	• 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

Role	Key Responsibilities
	• 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 • To accept responsibility in role modelling acceptable use of technology and social media to their children

Please note that, in line with the Department for Education document published in January 2018, "Searching, screening and confiscation: Advice for headteachers, school staff and governing bodies" (link here), staff may **lawfully search electronic devices**, without consent or parental permission, if there is a **suspicion** that the pupil has a device prohibited by School rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Any data, files or images that are believed to be **illegal** must be passed to the police as soon as practicable without deleting them.

Any data, files or images that are **not** believed to be **unlawful**, may be kept as evidence of a breach of the School's Behaviour Policy.

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 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, currently the Media Prefects, are used pre-emptively to discuss issues in the Lower Prep with small groups of pupils and they will be available 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 School website features information, resources, news and advice, for pupils, staff and parents.

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 Policy that may be required.
- Any upcoming initiatives that can be used to promote Online Safety throughout the School community.

Communication

"Communication" is split into 2 strands here: Email and Social Media. In all cases, **inappropriate use** includes the following:

- 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 another person'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 Harrodian.
- Using email to receive, forward or reply to messages intended to offend or 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 Harrodian, 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.
- Parents should not use School communication lists or platforms to advertise products and services, but could use our School platforms, Pinboard or SchoolNotices, instead.

Email

Harrodian 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.

Restriction

Access to and use of pupil email is a privilege accorded at the discretion of Harrodian. 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

Social networking applications include, but are NOT LIMITED to: Blogs, Online discussion forums, collaborative spaces, media sharing services, 'Microblogging' applications, Pinterest, photo sharing applications, chat rooms and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, Snapchat, YouTube, Flickr, Xbox Live, Blogger, Tumblr, Last.fm. These applications increasingly allow interaction between users who can "post", "comment", "share", "Tweet", "like", "pin", "friend", "unfriend ", and so on. Many of our principles surrounding social media also apply to other types of online presence such as virtual worlds but also messaging services like Whatsapp, an application that is often used by parents to communicate amongst themselves.

Pupils/ staff/ parents should not use Harrodian intellectual property unless it is being used to formally represent a School role. It is advised to meet with the Website and Communications Team before using names and logos which relate to the School.

Staff, pupils, parents, exam boards and software suppliers to the School increasingly want to harness these features for teaching, learning, communication, 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.

The following rules and guidelines cover interaction between staff, pupils and parents using such technologies:

Email

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

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 post derogatory, defamatory, offensive, harassing or discriminatory content or make disreputable comments about Harrodian
    - Staff should not initiate or accept "private" interactions and should keep personal information private
    - Staff should not use the Harrodian name or logo if their account is not used in a professional capacity
    - Staff should use a disclaimer when expressing personal views
    - Staff should report any negative comments/'trolling' to our website team before responding

- Pupils can post in public to a **Twitter** feed, to ask for clarification or further information
    - Pupils should not post derogatory, defamatory, offensive, harassing or discriminatory content or make disreputable comments about Harrodian
    - If pupils have a personal Twitter account, they must not use the Harrodian logo/name or branding for this

- Parents can post in public to a **Twitter** feed, to ask for clarification or further information
    - Parents should not post derogatory, defamatory, offensive, harassing or discriminatory content or make disreputable comments about Harrodian
    - If parents have a personal Twitter account, they must not use the Harrodian logo/name or branding for this
    - Parents should not use social media to air grievances or give negative feedback
    - Parents are advised not to post or tag photographs of Harrodian children (other than their own), unless permission has been granted

Google

- 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 *unlisted* and not publicly 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

- **Whatsapp:** used as a communication tool amongst parents, this application should be used for School-related matters only (such as homework, reminders, etc.) and not a platform for airing School grievances. In the case of any concerns, such as a School incident, parents should contact the School first before sending round any communication via Whatsapp.
- **Texting** a pupil (e.g. using *SMS, MMS, WhatsApp, Kik,* etc**.**) or calling their mobile phone should be avoided, unless, for Sixth Form students 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.

Use of Images

The School's use of images can be assumed to be acceptable, except when an opt-out request has been made in writing to Bronwen Lewis, Head of Administration. A letter outlining photo use is included in the Bulletin at the beginning of every academic year. Our guidelines covering image use are outlined in the section: "Mobile telephones, digital photography and use of images", below.

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. Remember to log off devices when not in use to ensure personal data cannot be seen by any other person. Any breaches of the Online Safety Policy by staff, pupils or parents will lead to appropriate action being taken.

Digital photography and use of images

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.

- **"No photographs list":** care should be taken to adhere to this list of pupils who do not give permission for photographs of them to be used (even for valid School uses such as School magazines).
- **Pupil use of devices to take photographs or video recordings**: this is banned unless supervised by a member of staff for a legitimate School purpose.
- **Staff use of devices to take photographs or video recordings:** this is not permitted on personal devices but is allowed for work-related purposes (assemblies, School magazine, website etc.) on School-owned devices such as the School cameras and School trip phones. These photos should then be deleted off the device and stored on secure network drives.
- **Image sharing:** staff should be able to share images of pupils for work-related purposes i.e. assemblies, website, newsletter and can be sent via websites like www.wetransfer.com as long as they are encrypted or password protected.
- **Social Media: staff should not share or upload student pictures for personal purposes or onto their own *personal* social media accounts.**
- **Tagging:** children are not to be tagged in photos and their surnames must not be published.
- **Photos taken on site:** parents should not share pictures or films containing images of Harrodian children other than their own, taken on the Harrodian premises, without permission from the parents of the children involved.

Mobile telephones

- **Mobile telephones:** these may not be used by pupils 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.
- Pupils in years below Year 7 (11s) must leave their mobile phone with Reception during the day (between 08:30 and 16:10).

Youth produced sexual imagery (YPSI or "sexting")

Harrodian will act in accordance with advice endorsed by DfE 'Sexting in schools and colleges: responding to incidents and safeguarding young people' (UK Council for Child Internet Safety 2016) 'Sexting in school and colleges'.

All incidents of youth produced sexual imagery (YPSI) will be dealt with as safeguarding concerns. The primary concern at all times will be the welfare and protection of the young people involved.

Young people who share sexual imagery of themselves or their peers are breaking the law. However, as highlighted in national guidance, it is important to avoid criminalising young people unnecessarily. Harrodian will therefore work in partnership with external agencies with a view to responding proportionately to the circumstances of any incident.

All incidents of YPSI should be reported to the DSLs as with all other safeguarding issues and concerns. Staff will not make their own judgements about whether an issue relating to YPSI is more or less serious enough to warrant a report to the DSLs. What may seem like less serious concerns to individual members of staff may be more significant when considered in the light of other information known to the DSLs, which the member of staff may not be aware of.

If staff become concerned about a YPSI issue in relation to a device in the possession of a student (e.g. mobile phone, tablet, digital camera), the member of staff will secure the device (it should be confiscated). This is consistent with DfE advice on searching, screening and confiscation: advice for headmasters, school staff and governing bodies (DfE January 2018), page 11 'After the search'. 'Searching, screening and confiscation'.

Staff will not look at or print any indecent images. The confiscated device will be passed immediately to one of the DSLs (see 'Viewing the imagery' below).

The DSL will discuss the concerns with appropriate staff and speak to the young people involved as appropriate. Parents and carers will be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm.

If, at any point in the process, there is concern that a young person has been harmed or is at risk of harm a referral will be made to SPA and/or the police immediately.

The police will always be informed when there is reason to believe that indecent images involving sexual acts and any child in the imagery is under 13 years of age.

The DSL will make a judgement about whether a reported YPSI incident is experimental or aggravated. Aggravated incidents involve criminal or abusive elements beyond the creation, sending or possession of sexual images created by young people. These include possible adult involvement or criminal or abusive behaviour by young people such as sexual abuse, extortion, threats, malicious conduct arising from personal conflicts, or creation or sending or showing of images without the knowledge or against the will of a young person who is pictured. Aggravated incidents of sexting will be referred to AfC's Single Point of Access for advice about whether or not a response by the police and/or children's social care is required.

This will facilitate consideration of whether:

- there are any offences that warrant a police investigation
- child protection procedures need to be invoked
- parents and carers require support in order to safeguard their children
- a multi-agency sexual exploitation (MASE) meeting is required
- any of the perpetrators and/or victims require additional support, this may require the initiation of an early help assessment and the offer of early help services.

Examples of aggravated incidents include:

- evidence of adult involvement in acquiring, creating or disseminating indecent images of young people (possibly by an adult pretending to be a young person known to the victim)
- evidence of coercing, intimidating, bullying, threatening and/or extortion of pupils by one or more other pupils to create and share indecent images of themselves
- pressure applied to a number of pupils (eg, all female pupils in a class or year group) to create and share indecent images of themselves
- pressurising a pupil who does not have the capacity to consent (e.g. due to their age, level of understanding or special educational needs) or with additional vulnerability to create and share indecent images of themselves

- dissemination of indecent images of young people to a significant number of others with an intention to cause harm or distress (possibly as an act of so-called 'revenge porn', bullying or exploitation)
- what is known about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage or are violent
- sharing of indecent images places a young person at immediate risk of harm, for example the young person is presenting as suicidal or self-harming

The DSL will make a judgement about whether or not a situation in which indecent images have been shared with a small number of others in a known friendship group with no previous concerns constitutes an aggravated incident or whether the School is able to contain the situation in partnership with all parents of the pupils involved, arrange for the parents to ensure that all indecent images are deleted and that the young people involved learn from the incident in order to keep themselves safe in future. In the latter instance, the DSL will consult with the police and the Single Point of Access to check that no other relevant information is held by those agencies and to ensure an agreed response is documented before proceeding.

Viewing the imagery

Adults should not view youth produced sexual imagery unless there is good and clear reason to do so. Wherever possible, the DSL's responses to incidents will be based on what they have been told about the content of the imagery.

Any decision to view imagery will be based on the DSL's professional judgement. Imagery will never be viewed if the act of viewing will cause significant distress or harm to a pupil.

If a decision is made to view imagery, the DSL will be satisfied that viewing:

- is the only way to make a decision about whether to involve other agencies (it is not possible to establish the facts from the young people involved)
- is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the young person or parent in making a report
- is unavoidable because a young person has presented an image directly to a staff member or the imagery has been found on a school device or network.

If it is necessary to view the imagery then the DSL will:

- never copy, print or share the imagery; this is illegal
- discuss the decision with the Headmaster
- ensure viewing is undertaken by the DSL with delegated authority from the Headmaster
- ensure viewing takes place with another member of staff present in the room, ideally the Headmaster, another DSL or a member of the Senior Leadership Team. The other staff member does not need to view the images
- wherever possible ensure viewing takes place on School premises, ideally in the Headmaster's or DSL's office
- ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the imagery
- record the viewing of the imagery in the pupil's safeguarding record, including who was present, why the image was viewed and any subsequent actions; and ensure this is signed and dated and meets the wider standards set out by Ofsted for recording safeguarding incidents

Deletion of images
If the school has decided that other agencies do not need to be involved, then consideration will be given to deleting imagery from devices and online services to limit any further sharing of the imagery.

The use of laptops in lessons

Harrodian 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.

Use of laptops in exams
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.

Laptops are permitted for **internal exams** at the discretion of the Learning Support Department and Form Teacher.

Harrodian 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 and their parents or guardians as part of its operation. Adhering to the guidelines in this Policy will help protect the security of this data (e.g. log off devices when not in use to ensure personal data cannot be seen by any other person). Please see the School's **Data Protection Policy** for further information as to the **rights** and **responsibilities** of all stakeholders.

What to do with concerns and incidents

For staff, pupils or parents: 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.
- **Do not reply** to any bullying/ trolling/ inflammatory remarks.
- 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 Website).
- Online Safety concerns may be reported anonymously to the Online Safety Coordinator via the SWGfL Whisper ***"Report an Issue"*** button on the Harrodian webpage.

Person responsible: Mr J Gledhill

Last update: October 2018
Next update: September 2019

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