HARRODIAN

Online Safety Policy

Contents

Objectives of the Policy

1. Define clear roles and responsibilities for online safety.
2. Provide guidelines for acceptable use of technology.
3. Establish monitoring and filtering standards.
4. Incorporate responsible iPad use into the broader online safety framework.
5. Educate pupils, staff, and parents on online safety practices.

Introduction

Harrodian recognises the integral role of Information and Communication Technology (ICT) in modern education. While offering significant opportunities, ICT presents associated risks. This policy addresses those risks and ensures the safe and appropriate use of all digital technologies, including iPads, by pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

Content: Being exposed to illegal, inappropriate, or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults to groom or exploit children.
Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
Commerce: Risks such as online gambling, inappropriate advertising, phishing, and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our School has created this policy to ensure appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Our Policy has been written by the School, in line with "Keeping Children Safe in Education" (KCSIE), "Teaching Online Safety in Schools", statutory PSHRE guidance and other statutory and guidance documents including, but not limited to:

- *Voyeurism (Offences) Act 2019*
- *The UK General Data Protection Regulation (UK GDPR)*
- *Data Protection Act 2018*
- *DfE (2023) 'Filtering and monitoring standards for schools and colleges'*
- *DfE (2021) 'Harmful online challenges and online hoaxes'*
- *DfE (2023) 'Teaching online safety in school'*
- *DfE (2022) 'Searching, screening and confiscation'*
- *DfE (2023) 'Generative artificial intelligence in education'*
- *Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'*
- *UK Council for Child Internet Safety: 'Education for a Connected World – 2020 edition'*
- *National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'*

- *DfE (2024) 'Keeping children safe in education 2024'*

It should be read in conjunction with the School's policies on behaviour, safeguarding, anti-bullying and data protection, and it complements curriculum subjects including Health, Relationships and Sex Education, Citizenship and Computing. It will be reviewed at least annually. Changes will be made immediately if technological or other developments so require. It will be published on the School website under "Policies", a summary relevant to staff will be published in the Staff Handbook and a summary relevant to pupils will be published in the Pupil Planner. Any inconsistencies should be brought to the attention of the Online Safeguarding Coordinator. Other information including Online Safety tips for staff, pupils and parents will also be posted on the School website. This policy operates in conjunction with School policies including, but not limited to:

- *Safeguarding and Child Protection Policy*
- *Behaviour Policy*
- *Anti-Bullying Policy*
- *Privacy Policy*
- *Code of Conduct for School Staff*
- *Relationships, Sex and Health Education Policy*
- *Search and Confiscation Policy*
- *Whistleblowing and Low Level Concern Policy*

Note that *Online Safety* and *Online Safeguarding* are used synonymously here. Previously the term "e-safety" has been used, but this is being phased out.

Roles and responsibilities

The following is a list of people who have roles and responsibilities relevant to Harrodian Online Safety. Note that external speakers mentioned in this section may not always be available to come into the School.

Role	**Key Responsibilities**
Head Master:	• Ensure that all online safety measures are **embedded** across policies, staff training, and curriculum planning. • To **support** the DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety. • To ensure that the Online Safeguarding Coordinator, Designated Safeguarding Leads and other staff receive suitable **training** to enable them to carry out their online safety roles and to train other colleagues as relevant. • To take **overall responsibility** for data and data security. • Working with the DSL and safeguarding governors to **update** this policy on an annual basis.

Designated Safeguarding Leads including: ● Head Designated Safeguarding Lead ● Pre-Prep Designated Safeguarding Lead ● Prep Designated Safeguarding Lead ● Senior and Sixth Form Designated Safeguarding Lead ● Online Safeguarding Coordinator	● To take day-to-day responsibility for **Online Safety** issues. ● Undertaking **training** so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online. ● To lead a "**safeguarding culture**", ensuring that Online Safety is integrated within the school community and that there is an awareness and commitment to Online Safety throughout the school community. ● To ensure that online safety **education** is embedded across the curriculum including remote learning. ● To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident. ● To monitor online safety incidents recorded on My Concern. ● To be aware of procedures to be followed in the event of a serious online safety incident. ● To **communicate** regularly with SLT and the Safeguarding Governors to discuss current issues and review incidents logged on My Concern. ● To be responsible for ensuring that all staff receive suitable **training** to carry out their safeguarding and online safety roles on a regular basis (at least annually). ● To liaise with the Local Authority and relevant agencies. ● To be updated regularly on online safety issues and legislation, and be aware of the potential for serious child protection issues arising from: ○ sharing of personal data ○ access to illegal/inappropriate materials ○ inappropriate online contact with adults/strangers ○ potential or actual incidents of grooming ○ cyber-bullying and the use of social media ● To liaise with school technical support staff and IT technicians ○ 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 understand the **filtering** and **monitoring** processes in place at the School and ensure that all safeguarding **training** given to staff includes an understanding of the expectations, roles and

	responsibilities in relation to filtering and monitoring systems at the school. ● To ensure a system is in place to monitor and support staff who carry out internal Online Safety procedures, e.g. network manager. ● To ensure that all relevant school **policies** have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them. ● To ensure the School website includes relevant information about online safety procedures. ● Working with the Headmaster and relevant responsible staff to update this policy on an annual basis.
Safeguarding Governors	● To ensure that this policy is effective and complies with relevant laws and statutory guidance. ● To ensure that the School follows all current Online Safety advice to keep the children and staff safe. ● Online safety practices are audited and evaluated, ensuring the effectiveness of the School's *Online Safety Policy* and procedures.
Online Safety Coordinator and Head of Computing	**Coordinate curriculum input** ● Liaise with other teachers in the department to cover the teaching of Online Safety in a progressive way **Coordinate extra-curricular training for pupils** ● In conjunction with the PSHE coordinator and Head of Sections, coordinate a program of visiting speakers. **Coordinate training for parents** ● Online Safety Coordinator to speak to parents of 11s and 12s at the beginning of the year. ● Parent rep to talk to parents of 8s **Arrange staff training** ● Ensuring all staff undergo online safety training at induction and at regular intervals. **Coordinate Safer Internet Day** ● Create a series of age-specific videos for further discussion. **Write, amend and publish Online Safety documents** ● Review the Online Safety Policy each year ● Review staff handbook entry. ● Review pupil planner entry ● Update documents and resources on the Harrodian.com website.

	Chair Online Safety Group ● Meetings (estimated 4 per year) will take place and include all Safeguarding leads, Heads of every Section in the School, the PSHE/ RSE/ Citizenship coordinator, and the IT Network Manager. ● Review Online Safety Incident Log. ● Discuss policy. ● Coordinate upcoming initiatives. ● Liaise with the student council. **Stay abreast of current developments in Online Safety** ● Attend relevant CPD courses (e.g. CEOP). ● Research, stay up-to-date and share information in the news, via Twitter hashtags, email newsletters, YouTube channels, etc. ● Continue with SWGfL 360degree safe review for risk assessment purposes. ● To undertake any other reasonable related tasks as requested by the Senior Leadership Team.
Network Management Team	● To report Online Safety related issues 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 regularly • 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. • That the use of School technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Online Safety coordinator and Headmaster ● 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. ● Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.

	• Ensuring that the Senior Leadership Team and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
Data and Information Managers	• To take overall responsibility for data management and information security ensuring that the School's provision follows best practice in information handling. • 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. • Undertake staff training relevant to GDPR.
Website managers	• To ensure the safeguarding of any children appearing on our public website by omitting surnames and any details. • Strictly adhere to the 'no photos' list of children. • To ensure that the Harrodian Twitter/X and Instagram accounts are 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 Agreement 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 practices when using digital technologies in and out of School.

Parents/Carers	• To 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, "Searching, screening and confiscation: Advice for headteachers, school staff and governing bodies", 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, or
- cause personal injury.

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, monitoring and education

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.

iPads

At the beginning of the academic year, September 2024, the School rolled out iPads to our 11s, 12s, and 13s. It is essential that the pupils follow the Pupil iPad Acceptable Use Agreement
Pupils should:

- Ensure iPads are fully charged daily and used only in cases approved by teachers.
- Respect privacy by avoiding unauthorised photography or video recording.
- Avoid attempts to bypass security settings or interfere with device management.

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 9 (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).

Filtering and monitoring

The School employs robust filtering and monitoring systems, including Mobile Device Management (MDM) for iPads. These measures:

- Prevent access to content deemed inappropriate, such as adult material, gambling, or extremist content.
- Track flagged activities, ensuring that concerns are addressed promptly.
- Maintain transparency with pupils and parents about monitoring practices.

Internet content and filtering and monitoring are reviewed on an on-going basis.

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.

To limit pupil exposure to risk from the School's IT systems, we have a strong and effective filtering system which is constantly monitored and managed by the School's firewall (Sonicwall) and overseen by the School's Network Manager.

Teaching staff are responsible for monitoring and reporting to the Online Safeguarding Coordinator any suspected misuse or problem associated with pupil use of School computers or other devices

With regards to Prevent Duty, content filters and monitoring aim to ensure that pupils are safe from terrorist and extremist material when they access the Internet.

With regards to filtering and monitoring systems, the School will ensure that:

- specific staff have assigned roles and responsibilities to manage systems
- staff know about the systems in place and how to escalate concerns
- there are annual reviews of the systems, or more frequently if there is a significant change or issue
- our safeguarding governors review the systems with the DSL, IT staff and service providers, to find out what more can be done to keep children safe
- the systems are effective for the age range of children and consider children potentially at greater risk of harm
- when we block online content, we attempt to ensure that it does not impact on teaching and learning
- filtering works across all devices, including iPads under school management and any mobile technology, when connected to the school network.

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.
- Peer mentors, currently the Media Prefects, are used preemptively 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.

Harrodian follows the DfE guidance detailed in the document: Teaching Online Safety in Schools.

Online Safety Group

A "Group", chaired by the Online Safeguarding Coordinator, and including Section Heads, the IT Manager, the PSHE Coordinator and Safeguarding Leads meets around 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" includes email and "social media", a term which covers any tool with a facility for sharing comments or "chatting". 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.

The School will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the *Anti-bullying Policy.*

Child-on-child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating, or encouraging sexual violence.
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks.
- Sexualised online bullying, e.g. sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery.
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse.

All staff will be aware of and promote a **zero-tolerance** approach to sexually harassing or abusive behaviour online.

The School will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress, and confusion.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the Internet. In some cases, a pupil may be groomed online to become involved in a wider network of

exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting, and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the Internet.

Where staff have any **concerns** about pupils with relation to CSE or CCE, they will bring these concerns to the **DSL** without delay, who will manage the situation in line with the *Safeguarding and Child Protection Policy.*

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the *Prevent Duty Policy*. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the *Prevent Duty Policy*.

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 the emails 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 the 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.

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 exclusion 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.

Mobile smart technology

The School recognises the usefulness of mobile smart technology (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.

Staff may not use their mobile phones for social use in the classroom, whilst on duty or whilst in the view of pupils. Admin staff must also restrict social use of their telephones – checking Instagram, Facebooks, etc. is not permitted during the working day. School telephones may not be used to make social/private calls unless in an emergency.

Whilst we recognise that it is useful for staff to use their phones to check School emails, take registers, etc. phones should be used sensitively and not in situations where they may jeopardise the safety and wellbeing of pupils, e.g. whilst on an observational duty.

Pupils are allowed to have mobile smart technology in School; however they must be switched off and stored away during the School day - 8.15am (Prep), 8.30am (Senior) to 4.00pm/4.10pm/4.55pm). Pupils may not use smart watches, e.g. Apple Watch, for communication during the school day. If a pupil needs to make a call urgently during the school day, they may go to the Admin Offices in either the Main Building or Senior School to use the telephone (if, however, the call is pertaining to sport, they should go to the Sports Department).

If a phone is being deliberately used on site without permission between 8.15am – 4.00pm (4.10pm Prep), the device will be confiscated and a detention set. The only exception is if permission has been granted for pupils to use their phones in lessons.

No pupils (including Sixth Form) can use their phones in the Prep Building. Phones may be confiscated if pupils are caught using them.

Sixth Form students are permitted to use their phones in School; however, use is limited to the Sixth Form areas and in the Café only.

Digital photography and use of images

- **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.
- **Permission** for the School to use images of children for valid school purposes is assumed, except when an opt-out request has been made in writing to the Head of Administration. A letter outlining photo use is included in the Bulletin at the beginning of every academic year, where a form for "opting out" is made available.
- Photographs for the **Harrodian School website** and other official publications, 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.
- **"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).
- **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 electronically 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.

Sharing nudes or semi-nudes

This is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. Alternative terms used by children and young people may include 'dick pics' or 'pics'. It is a form of child sexual abuse. All incidents will be dealt with as safeguarding concerns. The primary concern at all times will be the welfare and protection of the children 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.

Concerns about nudes or semi-nudes

If there are concerns about the sharing of nudes or semi-nudes, the following procedures will be applied:

- Concerns must be reported to the designated safeguarding leads (DSLs) immediately using MyConcern.
- Imagery should not be viewed, copied, printed, shared, stored or saved neither should the young person be asked to share or download the imagery - this is illegal.
- If the imagery has already been viewed by accident (e.g. if a young person has shown it before they could be asked not to), this must be reported to the DSL
- The imagery should not be deleted nor should the young person be asked to delete it.
- The young person(s) involved in the incident should not be asked to disclose information regarding the imagery as this is the responsibility of the DSL.
- Information about the incident should not be shared with other members of staff, the young person(s) it involves, or their, or other, parents and/or carers.
- At this stage, nothing will be said or done to blame or shame the young person involved. However, it is important to explain to the young person that there is a need to report the incident and to offer reassurance that they will receive support and help from the DSL.

Staff reserve the right to confiscate a device in the possession of a pupil if they have concerns about sharing nudes or semi-nudes in relation to the device. This is consistent with the government's Searching, screening and confiscation: advice for schools guidance.

The DSL will follow the government's Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance. Once they are aware of an incident, the DSL will hold an initial review meeting with appropriate staff. This may include the staff member(s) who heard the disclosure and the safeguarding or leadership team who deal with safeguarding concerns.

The initial review meeting will consider the initial evidence and aim to establish

- whether there is an immediate risk to any child or young person
- if a referral should be made to the police and/or children's social care
- if it is necessary to view the image(s) in order to safeguard the child or young person – in most cases, images or videos should not be viewed
- what further information is required to decide on the best response
- whether the image(s) has been shared widely and via what services and/or platforms. This may be unknown

- whether immediate action should be taken to delete or remove images or videos from devices or online services
- any relevant facts about the children or young people involved that would influence risk assessment
- if there is a need to contact another education setting or individual
- whether to contact parents or carers of the children or young people involved – in most cases they should be involved

The DSL will make an immediate referral to the police and/or children's services if

- the incident involves an adult
- there is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
- what they know about the images or videos suggests the content depicts sexual acts that are unusual for the young person's developmental stage, or are violent
- the images involve sexual acts and any pupil in the images or videos is under 13
- they have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, if they are presenting as suicidal or self-harming

If none of the above applies, the School can decide to respond to the incident without involving the police or children's services. The incident may be escalated at any time if further information/concerns are disclosed at a later date. First, the DSL will be confident that they have enough information to assess the risks to any child involved and the risks can be managed within our School's pastoral support, behaviour procedures and, if appropriate, the local network of support.

The DSL will contact children's services if any child or young person involved is already known to them. If, because of the investigation, the DSL believes there are wider issues that meet the threshold for children's services' involvement, they will make a referral in line with this policy and local safeguarding procedures.

Viewing the imagery

The decision to view any imagery will be based on the professional judgement of the DSL and will comply with this policy. 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 because it is not possible to establish the facts from any child or young person involved
- is necessary to report it to a website, app or suitable reporting agency (such as the IWF) to have it taken down, or to support the child, parent or carer in making a report
- is unavoidable because a child or young person has presented it directly to a staff member or nudes or semi-nudes have been found on a School device or network

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 to limit any further sharing. This decision will be based on the DSL's judgement in line with the guidance.

The use of laptops in lessons and examinations

The permission to use laptops (word processors) at Harrodian is managed by The Learning Enrichment Department. All pupils in the Pre-Prep, Prep and Senior Schools who require the use of a laptop must attain a Laptop Passport from Learning Enrichment to be allowed to use a laptop in the classroom and examinations.

If a Laptop Passport is awarded, a member of the Learning Enrichment team will go through a Laptop Passport Checklist and Contract with the child - this includes points relating to behavioural expectations when using a laptop in class. Teachers will then be notified that the child may use a laptop in the classroom and in examinations.

Use of a laptop or word processor in examinations is a formal access arrangement/reasonable adjustment, in accordance with guidance from the Joint Council for Qualifications (JCQ).

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).

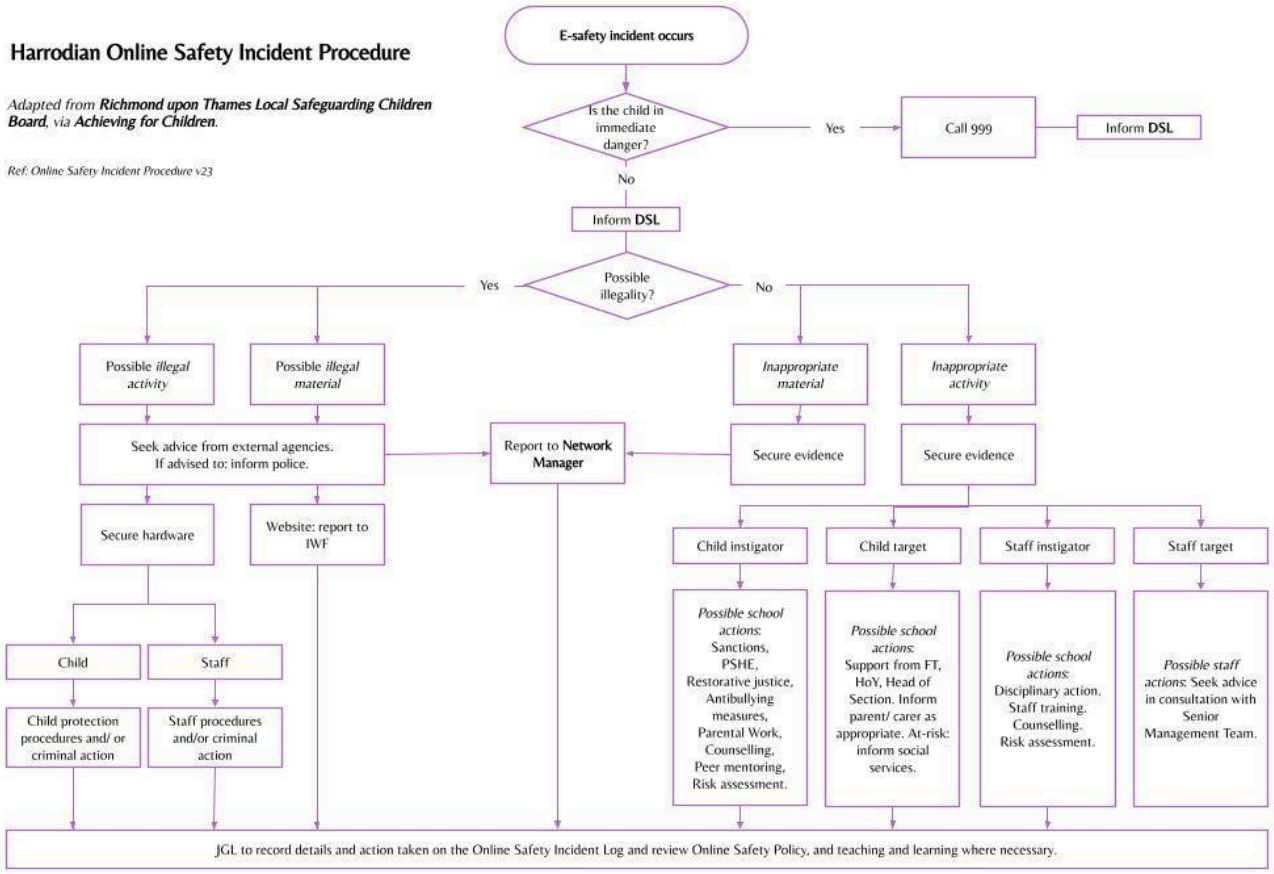
What to do with concerns and incidents

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

For staff, pupils or parents: if you are made aware of an Online Safety incident, please inform one of the school's DSLs (Designated Safeguarding Leads). 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. Steps taken should be recorded on MyConcern and tagged "Online Safety". 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 try Childnet as a useful first port of call for all concerns (also linked from the Harrodian website).
- Online Safety concerns may be reported anonymously via worry boxes in the School.

Approved by:	Senior Leadership Team
Last reviewed:	March 2025



Here is a link to the Harrodian Online Safety Incident Procedure.

Appendix A

Current Online Safeguarding Trends

In accordance with Ofsted's "School Inspection Handbook", we assume, as Ofsted inspectors do, that: "*sexual harassment, online sexual abuse and sexual violence are happening in the community, and potentially in the school, even when there are no specific reports, and put in place a whole-school approach to address them.*"

In our School over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students: meanness, bullying and abuse via Snapchat and TikTok; inappropriate use of phones, for example to film and photograph in class, at break or even in the toilets; and partisan views about the conflict in Israel/Gaza.

Self-generative artificial intelligence has been a significant change, with students having often unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers and above all safety: none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. We at Harrodian need not only to tackle this in terms of what comes into school but also educate young people and their parents on use of these tools in the home.

Ofcom's '*Children and parents: media use and attitudes report 2023*' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often ignored.

Statistics relevant to Pre-Prep and Lower Prep (source: LGfL) include: 20% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases found (of this same kind where the abuser is not present).

Statistics relevant to Upper Prep and Seniors (source: LGfL) include: 95 percent of students have their own mobile phone by the end of Year 7, and the vast majority do not have safety controls or limitations to prevent harm of access to inappropriate material. This is particularly pertinent given that 130,556 cases of self-generated child sexual abuse material were found of 11-13 year olds (Internet Watch Foundation Annual Report). These were predominantly (but importantly not only) girls; it is important also to recognise more and more older teenage boys being financially extorted after sharing intimate pictures online. In the past year, more and more children and young people used apps such as Snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news. The 2023 Revealing-Reality: Anti-social-Media Report highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons. At the

same time, the Children's Commissioner revealed that ever younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which has had a significant influence on many young boys over the past year which schools have had to counter. From the many schools that LGfL spoke to over the past year, there was a marked increase in the number having issues with fights being filmed and shared, a disturbing increase in the cases of self-harm, and sexual abuse being coerced with threats of violence (many even in primary schools). There has been a significant increase in the number of fake profiles causing issues in schools, both for the school, where the school logo and/or name have been used to share inappropriate content about students and also spread defamatory allegations about staff, and also for students, including where these fake profiles are used to bully others (sometimes pretending to be one student to bully a second student).

Appendix B

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:

General

- Staff, pupils and parents should not post derogatory, defamatory, offensive, harassing or discriminatory content or make disreputable comments about Harrodian, or when recognisable as a member of the Harrodian community. It is not suitable for parents to use social media to air grievances or give negative feedback. Negative comments or trolling should be reported to our website team.

- If staff, pupils or parents use a personal social media account, they must not use the Harrodian name, logo or other branding for this.

- Staff, pupils and parents are advised not to post or tag photographs of Harrodian children unless permission has been granted.

Staff may only use certain approved social media platforms to facilitate their role, improve communication or enable them to fulfil exam board requirements:

X (formerly known as Twitter)

- Staff can post in public to an **X** feed. 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 and should keep personal information private.

- Staff should use a disclaimer when expressing personal views.

Google

- Staff may communicate with pupils using **Google Classroom** to share and mark work, and to conduct remote lessons. Standards of professionalism by staff and courtesy by pupils should match levels of face-to-face communication and be guided by the same principles of communication as email and other online tools as detailed in this policy.

- Staff may use **YouTube** (a Google site) to host videos relevant to school work, sports, extra-curricular work, drama, or other valid purpose, with the following caveats:
    - Content featuring pupils should be *unlisted* and not publicly viewable or searchable.
    - Current pupils may be provided with a link to the video as required.
    - Staff should ensure that there are no pupils from the “no photos” list featured in videos.

- Staff may use **Google Productivity Apps** to share, and collaborate on documents, spreadsheets, presentations, etc.

- 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 should not be used as 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.

- 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 notice board 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 breach of the Online Safety Policy by staff, pupils or parents will lead to appropriate action being taken.