

# HEADG ONLINE SCHOOL UK

## **e-Safety Policy**

The foundation of HeadG Online School is based on technology and the use of the internet. The safe and responsible use of the internet and technology, by the children and young people who attend HeadG Online School, is one of our top priorities. E-safety encompasses internet technologies and electronic communications such as mobile devices and wireless technology. HeadG Online School is committed to educating children and young people about the benefits and risks of using technology and provides safeguards and awareness for pupils to enable them to control and monitor their online experiences. It is also important that pupils of HeadG Online School are knowledgeable of the ways they can report unwanted online behaviour (in and out of school) and misuse of school platforms.

### **Purpose**

At HeadG Online School, we consider our educational establishment to be our online platforms, which are all accessed via the internet: Adobe Connect, Canvas and iSAMS. Our platforms are used to facilitate communications, raise educational standards, promote pupil achievement, support the professional work of staff and enhance the school's management information and administration systems.

As the basis of our school and also as part of the curriculum, the internet is a necessary tool for teaching and learning. It is essential for life in the twenty-first century: for education, for business and for social interaction. Access to the internet is necessary for attendance to HeadG Online School and is an entitlement for those who show a responsible and mature approach to its use.

Our pupils will inevitably access the internet outside of school time and should be educated in how to evaluate online information and to take care of their own safety and security online and when using technology. We believe that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

The purpose of the HeadG Online School e-Safety policy is to:

- Safeguard and protect all members of our community online
- Identify approaches to educate and raise awareness of e-Safety throughout the community
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to e-Safety concerns

HeadG Online School identifies that the issues within the realms of e-Safety are considerable; however, these can be broadly categorised into three areas of risk:

- **Content** : being exposed to illegal, inappropriate, harmful material
- **Contact** : being subjected to harmful online interaction with other users
- **Conduct** : personal online behaviour that increased the likelihood of, or causes, harm

## **Roles and Responsibilities**

### **a. Senior Leaders**

The Director, Heads and Deputy Heads of School will:

- Ensure that e-Safety is viewed as a safeguarding issue and that practice is in line with national recommendations and requirements
- Ensure there are appropriate and up-to-date policies regarding e-Safety, including the Behaviour policy, which covers acceptable use of school platforms
- Recommend to families that appropriate filtering systems are in place in the home of the young people who attend lessons
- Ensure that e-Safety is embedded in the curriculum, which enables the children and young people to develop an age-appropriate understanding of e-Safety
- Support each other in their roles so that they have sufficient time to fulfill their safeguarding responsibilities
- Ensure that there are robust reporting channels for the community to access regarding e-Safety concerns including internal and national support
- Audit and evaluate e-Safety practice to identify strengths and areas for improvement
- Act as points of contact on all online safeguarding issues and liaise with other members of staff and external agencies, as appropriate
- Work alongside the school's DSL/CPO to ensure e-Safety is recognised as part of the school's safeguarding responsibilities
- Ensure that members of staff receive up-to-date e-Safety training
- Access appropriate training to ensure they recognise the additional risks that pupils with SEN and disabilities may face online
- Keep up-to-date with research, legislation and trends regarding e-Safety
- Ensure that e-Safety is promoted to parents, carers and families through a variety of approaches
- Maintain records of e-Safety incidents as well as the actions taken as part of the school's safeguarding procedures

- Monitor e-Safety incidents to identify gaps and use this data to update the response, policies and procedures of the school
- Work to ensure the relevant updates are made to the policy, where appropriate

#### **b. Individual Staff Members**

It is the responsibility of all members of staff to:

- Read and adhere to the e-Safety policy
- Ensure that only authenticated users of HeadG Online School platforms are permitted into live lessons, with no access to 'guests' (unauthenticated users)
- Ensure strong passwords are utilised, two-factor authentication is used where required and passwords are not shared with others
- Ensure passwords are changed regularly and/or when prompted
- Take responsibility for the security of school systems and the data they use or have access to
- Model good practice when using technology and maintain a professional level of conduct in their use of technologies
- Embed e-Safety education in curriculum delivery, wherever possible
- Have an awareness of a range of e-Safety issues and how they may be experienced by the children and young people
- Identify e-Safety concerns and take appropriate action by following the school's safeguarding policies and procedures
- Know when and how to escalate e-Safety issues, including signposting the appropriate support
- Take responsibility for professional development in this area

#### **c. Pupils**

It is the responsibility of pupils (at a level appropriate to their age and ability) to:

- Engage in age appropriate e-Safety education opportunities
- Read and adhere to the rules regarding the use of the school's online platforms
- Safely and responsibly use the Adobe and Canvas to support learning
- Respect the feelings and rights of others online (and offline), in and out of school
- Take responsibility for keeping themselves and others safe online
- Seek help from a trusted adult, if there is a concern online or while using school platforms, and support others that may be experiencing e-Safety issues

- Not to engage in the personal use of technology and the internet, i.e. gaming consoles or social media, during timetabled classes

#### **d. Parents and Carers**

It is the responsibility of parents/carers to:

- Read the school handbook, behaviour and e-Safety policy and to encourage their child or young person to adhere to them
- Support the school's e-Safety approaches by discussing e-Safety issues with their child or young person and reinforcing appropriate and safe online behaviour outside of school
- Role model safe and appropriate use of technology and social media
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the school and other appropriate agencies if they or their child encounter risk or concerns online
- Use school systems i.e. the Parent Portal and Canvas in a safe and appropriate way
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies
- Adhere to the rules of the HeadG Online School Parent Community on Facebook (if a member of this group)

### **Education and Management Approaches**

#### **a. Education and Engagement with Pupils**

HeadG Online School will establish and embed e-Safety into the curriculum to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring pupils engage in age appropriate education regarding safe and responsible use of the internet
- Including e-Safety in PSHE classes, in assemblies and House meetings and also in computing-specific classes
- Reinforcing e-Safety messages regularly during lessons, particularly when pupils are undertaking independent research activities
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

HeadG Online School will support pupils to read and understand e-Safety education materials by:

- Displaying e-Safety materials on class pages and during lessons
- Informing pupils that their use of school platforms is monitored for safety and security purposes and in accordance with legislation
- Rewarding the positive use of technology
- Providing e-Safety education during the transition phase between KS2 and KS3, for Year 6 to Year 7
- Seeking pupil voice when creating and implementing rules in the classroom
- Using support, such as external bodies, where appropriate to complement and support internal e-Safety education approaches

#### **b. Training and Engagement with Staff**

HeadG OnInie School will:

- Provide and discuss e-Safety policy and procedures with staff members
- Provide up-to-date information to all staff members, which covers the potential risks posed to pupils under the 'content, contact conduct' categories
- Make staff aware that our platforms are monitored and that activities can be traced to individual users. Staff will be reminded to conduct themselves in a professional manner and in accordance with our school policies when accessing the relevant platforms
- Make staff aware that their online conduct outside of the school setting, including the personal use of social media, could have an impact on their professional role and reputation
- Highlight educational resources and tools which staff could use, according to the age and ability of the pupils
- Ensure all members of staff are aware of the procedures to follow regarding e-Safety concerns affecting children, young people and the wider HeadG OnInie School community

### **c. Awareness and Engagement with Parents/Carers**

Parents/carers have a fundamental role to play in enabling their child or young person to become a safe and responsible user of the internet and technologies.

HeadG OnInie School will build a partnership approach to e-Safety with parents and carers by:

- Providing information and guidance on e-Safety
- Draw their attention to the e-Safety policy and expectations in newsletters, the school handbook, the prospectus and the school website
- Requesting that parents/carers read e-Safety information as part of joining the HeadG Online School community
- Request that parents/carers discuss responsible use of school platforms, when joining the school and between each school year
- Requesting that parents/carers regularly discuss e-Safety with their child or young person at home, including the implications of unsafe or irresponsible behaviours

### **Reducing Online Risks**

The internet is a continually changing environment with new programmes, platforms, software, devices, website and material being created at a rapid pace. With this in mind, HeadG Online School will:

- Regularly review the school's use of technology and the internet to identify, assess and minimise online risks
- Examine emerging technologies for educational benefit and carry out appropriate risk assessments before use by the school
- Ensure that appropriate materials are posted on school platforms, with pupils and families advised to use filtering and monitoring on their own devices and to ensure reasonable all precautions are taken so that pupils only access appropriate material

It should be noted that due to the interconnectivity of the internet, it is not possible to guarantee that unsuitable material will not be accessed by children and young people accessing the internet, while schooling with HeadG Online School, in their homes.

All members of the HeadG Online School community have the school's expectations regarding safe and appropriate behaviour online communicated to them. With this, the importance of not posting any content, comments, images, videos which could cause harm, distress or offence to other members of the community is made known. This is also highlighted in the education of our pupils, teachers and staff.

## **Safer Use of Technology**

### **a. Classroom Use**

HeadG Online School requires pupils to use technology and the internet to participate in their day-to-day schooling. This includes, but is not limited to access to:

- Adobe video conferencing
- Canvas (virtual learning environment)
- Google Drive
- Personal email (i.e. Outlook, Gmail)
- Educational websites and platforms (i.e Quizlet, Kahoot, ActiveLearn)
- Computers, laptops, tablets and other mobile/digital devices

All school-owned platforms will be used in accordance with our behaviour policy, safeguarding policy and teacher standards and expectations, with appropriate safety and security measures in place.

Members of the HeadG Online School team will evaluate websites, learning tools and applications fully prior to use in the classroom or before recommending these for use outside of school.

Pupils are strongly advised to use age appropriate search tools, with parents ensuring that appropriate filtering is enabled.

Members of the HeadG Online School community will ensure that all internet-derived materials complies with copyright law and that sources of information are acknowledged.

To the best of their ability, teachers are able to and will supervise pupils when using school platforms. Teachers cannot oversee any other websites and applications that may be accessed during lesson time, against our school rules and against teacher recommendations.

### **b. Managing Access**

HeadG Online School will maintain a written record of users who have access to all school platforms and systems. All members of the HeadG Online School community are expected to adhere to the policies and procedures in place to keep everyone safe online and when using technology.

### **c. Filtering and Monitoring**

Pupils at HeadG Online School access lessons from home and there is limited ability of staff members to prevent pupils from accessing websites that the school does not deem appropriate for children and young people. We request the cooperation of parents and carers to monitor the online activity of their child or young person. HeadG Online School will use websites, applications and programmes that are appropriate to the age and experience of pupils. The school recommends that this should continue into the home when utilising technologies and the internet outside of school time.

Filtering and monitoring of children and young people's online activity is strongly recommended to parents, carers and families. Staff and pupils who discover that an unsuitable site has been shared or posted on school platforms must be reported to a member of Senior Leadership.

The school will report any online material it believes to be illegal to the appropriate agencies i.e. IWF or Child Exploitation and Online Protection command (CEOP).

HeadG online School recognises the existence of the [Internet Watch Foundation](#) list and would encourage parents and carers to ensure their child or young person is not accessing the sites mentioned.

Parents and carers will be informed of any breaches of behaviour, safeguarding, anti-bullying and e-Safety policies involving their child or young person.

HeadG Online School is aware that pupils, parents and carers cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

### **d. Managing Personal Data Online**

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.



#### **e. Security and Management of Information Systems**

HeadG Online School will take appropriate steps to ensure the security of our platforms and information systems, including:

- Encryption of video conferencing platforms (Zoom)
- Virus protection is up to date on office technologies
- Using cloud storage platforms for the storage of files, as opposed to using portable media storage
- Not downloading software from untrustworthy sources to work devices or opening unfamiliar email attachments
- Regularly check files on devices and deleting as appropriate
- Ensure users are utilising appropriate login details and passwords for access to school platforms
- Use of two-factor authentication for access to iSAMS (MIS)
- All users using work devices or using school platforms are expected to log off or lock their screens/devices if systems are unattended

#### **f. Password Policy**

All members of the HeadG Online School team have their own unique username and passwords to access our systems: Adobe, iSAMS and Canvas. Office staff have unique usernames and passwords for their HeadG Online School email. Members of staff are required to keep their passwords private.

All pupils use unique login details to access Adobe and Canvas and parents will utilise unique login details for access to the parent portal and Canvas. Pupils and parents are required to keep their passwords private.

HeadG Online School advises and requires members to:

- Use strong passwords (including alphanumeric, case-sensitive passwords)
- Change passwords regularly and/or when prompted by platforms
- Not share passwords with others or leave passwords written down where others can find it
- Not login as another user at any time

#### **g. Managing the Safety of the MOS Community**

Staff or pupil's personal information will not be published on our school website; the contact details on the website will be the address, email and telephone number of our main office.

Any administrator accounts for school platforms and the website will be secured with an appropriately strong password.

We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

#### **h. Publishing Images and Videos Online**

We will ensure that all images and videos shared online are used in accordance with the associated policies, including, but not limited to our behaviour policy and safeguarding Policy.

#### **i. Managing Email**

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies including, but not limited to our behaviour policy and safeguarding policy.

Any electronic communication which contains sensitive or personal information will only be sent using email platforms that are protected by strong login credentials.

School email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell the Senior Leadership if they receive offensive communication, and this will be recorded in the school's safeguarding files or records.

All members of the school office staff are provided with an email address to use for all official communication.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

Excessive social email use can interfere with teaching and learning and productivity. Teachers and staff members are asked to avoid sending personal emails during times of active working and contact time, excluding break times.

#### **j. Use of Video Conferencing (Zoom)**

One of HeadG Online School's main platforms is Adobe, which is used to conduct our live, interactive lessons. As a paid service, the school has access to heightened security features that are not in place on the non-paid version of the platform. In using Adobe, HeadG Online School will ensure that:

- Only authenticated users will be permitted to enter live classes
- Teachers have control over who can enter live classes via the waiting room
- Teachers are always visible on webcam as per the teacher standards and expectations policy
- All lessons are recorded for safeguarding purposes, lesson observations and for later review by pupils
- Pupils have a choice of how they engage with their online lessons: to communicate via the chat box only, verbally and with the chatbox, the chat box and webcam, or verbally with the chat box and webcam. All combinations are acceptable to meet the needs of pupils
- Teachers have the ability to turn off the webcams and microphones of pupils, one at a time or in bulk
- Teachers have the ability to control who is sharing their screen and annotating documents/images
- Pupils are able to communicate the teacher publicly or privately during live lessons
- Pupils are not able to participate in 'instant meetings' with one another
- Only authenticated users are permitted to access lesson recordings, posted on the Canvas class pages
- Only key administrators will be given access to Adobe admin control functions
- The unique login and password details for Adobe should be kept securely, to prevent unauthorised access

By enrolling with HeadG Online School, parents and carers consent to their child or young person participating in video conferencing via Adobe, including the use of chat, webcam and microphone functions.

#### **k. Use of Virtual Learning Environments (Canvas)**

HeadG Online School uses Canvas as its official online learning environment (LMS).

Senior Leadership and teachers will continually monitor the use of Canvas in their day-to-day workings, including the use of messaging features and discussion forums.

Only current members of staff, pupils and parents will have access to Canvas.

When staff, pupils and parents leave the school, their account will be disabled and stored in Canvas.

Pupils and staff will be advised of appropriate usage of the Canvas platform in our behaviour policy, school handbook and through our teacher standards and expectations.

All Canvas users should be mindful of using copyrighted materials. Staff and pupils should make use of 'Canvas Commons' which contains materials covered by Creative Commons regulations. Stock images should be used, where possible.

Any concerns regarding the content of Canvas will be recorded and handled in the following ways:

- Pupils or staff members will be asked to remove any material deemed to be inappropriate or offensive
- If the pupil or staff member does not comply, the material will be removed by the site administrator
- Access to the Canvas may be suspended
- The pupil or staff member will discuss the issues with a member of senior leadership before reinstatement of access
- A pupil's parents/carers may be informed
- If the content is illegal, HeadG Online School will respond in line with existing child protection procedures and contact the relevant agencies, including the police, where necessary

A visitor may be invited onto Canvas by a member of the senior leadership; in this instance, there may be an agreed focus or a limited time slot i.e. during inspection proceedings

## I. Management of Databases Storing Pupil Data and Records (iSAMS)

HeadG Online School uses iSAMS as our management information system (MIS) for storing pupil data, including contact information, academic progress, pastoral notes, as well as being used for contact with parents and carers.

Heads of School and members of the office team are responsible for maintaining the information held on pupils, enrolled and unenrolled.

iSAMS is used by HeadG Online School in accordance with data protection legislation, including GDPR.

To ensure pupil data is protected:

- Only authorised members of the HeadG Online School team will have access to the information held on pupils
- Authorised users of iSAMS will only be provided with the information that permits them to complete their day-to-day duties
- Two-factor authentication will be utilised to access the iSAMS platform by all staff
- All members of staff at HeadG Online School will be advised about the appropriate safety measures, including the use of strong passwords, not sharing passwords, and locking or logging out of the system when not in use
- Parents and carers will be informed of the expectations regarding use of the Parent Portal (which uses iSAMS as its platform), including the use of strong passwords, not sharing passwords and logging out of the portal when not in use

## **Social Media**

HeadG Online School recognises that social media can be a powerful tool for communication and can be a positive force in terms of communication and marketing. Conversely, if not used in a considered, safe and responsible way, negative consequences can result. HeadG Online School highlights the following expectations and recommendations regarding the use of social media by members of the school community.

### **a. Expectations**

The expectations regarding safe and responsible use of social media applies to all members of HeadG Online School.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of the HeadG Online School community are expected to engage in social media in a positive, safe and responsible manner.

All members of the HeadG Online School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

Concerns regarding the online conduct of any member of the HeadG Online School community on social media, should be reported to the Director or a member of Senior Leadership and will be managed in accordance with our school policies that are in place for the safety and wellbeing of our pupils.

### **b. Use of Social Media by Staff Members**

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated, as required, via regular staff training opportunities.

The reputation of HeadG Online School and all members of our community is important to us. All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.

Action may be taken if staff members are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media platforms. This includes, but is not limited to:

- Setting the privacy levels of their personal sites
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the school

Members of the HeadG Online School community are recommended not to identify themselves as a member of staff, at the school, on their social media profiles or accounts. This will safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the Director or Senior Leadership immediately if they consider that any content shared on social media sites conflicts with their role.

### **c. Communicating with Pupils and Parents/Carers**

All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles.

Any pre-existing relationships or exceptions that may compromise this, will be discussed with the Director or Senior Leadership

If ongoing contact with pupils is required once they have left the school, members of staff will be expected to use existing platforms or channels.

Members of staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Director or Senior Leadership.

Any communication from pupils and parents/carers received on personal social media accounts will be reported to the Director or Senior Leadership.

#### **d. Use of Social Media by Pupils**

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources. Resources on the safe use of social media and other platforms is posted via the school's social media platforms, advocating for safe and responsible use of social media sites and gaming platforms.

Any concerns regarding a pupil's use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and safeguarding. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

HeadG Online School recommends to pupils:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
- To use strong passwords and not to share these with friends
- To use social media sites which are appropriate for their age and abilities
- To block and report unwanted communications
- To report concerns to a trusted adult, either at home or at HeadG Online School

#### **e. Official Use of Social Media**

HeadG Online School utilises social media for marketing and for communication with our community.

The official use of social media sites only takes place with clear educational, marketing or community engagement objectives, with specific intended outcomes.

Leadership staff have access to account information and login details for our social media channels.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.



Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:

- Always be professional and aware they are an ambassador for the school
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared
- Always act within the legal frameworks they would adhere to within the workplace including: confidentiality, copyright, data protection and equalities
- Ensure that they have appropriate consent before sharing images on the official social media channels
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so
- Inform the Director or a member of Senior Leadership of any concerns, such as criticism, inappropriate content or contact from pupils

### **Use of Personal Devices and Mobile Devices**

HeadG Online School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but we strongly advocate for technologies being used safely and appropriately when schooling and in the school community.

Our pupils access lessons from home and there is limited ability for staff members to prevent pupils from utilising their personal devices for means other than those that support learning, during lessons.

HeadG Online School expects that pupils' personal devices and mobile phones should be kept to one side during lessons. Mobile phones or personal devices will not be used by pupils during lessons or formal educational time unless as part of an approved and directed curriculum-based activity, as advised by a member of the teaching team. We greatly appreciate the support of our parents and carers of their cooperation in supporting our stance on this.

Mobile phones and other personal devices should not be used during assessments and examinations. Pupils found to have used their devices to gain advantage in any assessments or examinations may result in no award being presented to the pupil.

Parent Liaison, Heads of School or other members of Senior Leadership will be in contact with parents/ carers where concerns arise regarding the inappropriate use of personal devices and mobile phones which contravenes our policies, including: behaviour, e-safety, safeguarding, and anti-bullying policies.

HeadG Online School will act in accordance with the sanctions outlined in the aforementioned policies and will inform the relevant external bodies and authorities if there is a suspicion that any illegal or criminal offences have taken place.

### **Responding to e-Safety Incidents and Concerns**

All members of the HeadG Online School community should report any online safety concerns, including (but not limited to): cyberbullying, accessing inappropriate content, abusive messaging or sharing of harmful imagery, and illegal content. These should be reported to the Director or another member of Senior Leadership.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Pupils, parents and staff will be informed of our complaints procedure.

Any incidents or concerns will be recorded electronically for reference if required at a later date.

The school will inform parents/carers of any online safety incidents or concerns involving their child, where required.

We require all members of the community to work in partnership to resolve online safety issues. After any investigations are completed, the school will identify any lessons learnt and implement any policy or curriculum changes, as required.

If the Director or Senior Leader(s) are unaware of how to proceed with a concern or incident, advice and guidance will be sought from the necessary external bodies and organisations.

Where there is suspicion that illegal activity has taken place, the Director or Senior Leader(s) will contact the necessary local authority or body, will contact the police (on 101 or 999, in the UK) if there is an immediate danger or risk of harm.

## **Procedures for Responding to Specific Online Incidents or Concerns**

### **a. Online Sexual Violence and Harassment Between Children and Young People**

HeadG Online School recognises that sexual violence and sexual harassment between children and young people can take place online. Examples may include; non-consensual sharing of sexual images and videos sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

The school recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

The school also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

The school will ensure that all members of our community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children and young people by implementing a range of age and ability appropriate educational methods as part of our PSHE curriculum.

We will ensure that all members of our community are aware of sources of support regarding online sexual violence and sexual harassment between children and young people.

We will respond to concerns regarding online sexual violence and sexual harassment between children and young people, regardless of whether the incident took place on our platforms or otherwise.

If we are made aware of online sexual violence or sexual harassment, the school will:

- Immediately notify the CPO/DSL and act in accordance with our behaviour, safeguarding, e-safety, or anti-bullying policies
- Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support
- Implement the appropriate sanctions as outlined in our behaviour policy
- Inform parents/carers, if appropriate, about the incident and how it is being managed
- If appropriate, make a referral to external agencies, such as Children's Social Services and/or the Police

- If a criminal offence has been committed, the school will discuss this with the child or young person's local police authority first to ensure that investigations are not compromised
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate

#### **b. Youth Produced Sexual Imagery**

HeadG Online School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the CPO/DSL/Senior Leadership.

The school will liaise with the relevant national guidance, for example, '[Sexting in schools and colleges: responding to incidents and safeguarding young people](#)' for information on youth produced sexual imagery and how to respond to this.

The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on school platforms or personal equipment.

HeadG Online School will not:

View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so - If it is deemed necessary, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented

Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so

If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with the relevant school policies i.e. safeguarding
- Ensure we proceed in line with the guidance in '[Sexting in schools and colleges: responding to incidents and safeguarding young people](#)'

- Block access to all users and isolate the image, where the image has been taken or shared on school platforms
- Consider the risks to and the vulnerability of the pupil(s) involved, including carrying out checks with other agencies
- Inform parents and carers, where appropriate, about how the incident is being managed
- Make a referral to the relevant Children's Social Services and/or the Police
- Provide the necessary support for pupils, including counselling and pastoral support
- Implement appropriate sanctions in accordance with our Behaviour Policy but taking care so not to further traumatise victims where possible
- Consider deletion of the images, where advised and/or in line with national guidance
- Delete images only when the DSL/CPO has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation
- Review the handling of the incident, ensuring that any changes are implemented effectively to maintain best practice

### **c. Online Sexual Abuse and Exploitation**

HeadG Online School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

The school recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL/CPO.

We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation).

If the school are made aware of an incident involving sexual abuse and exploitation, we will:

- Act in accordance with the relevant school policies i.e. safeguarding
- Make a referral to Children's Social Services (if appropriate) and to inform the police (via 101 or dialling 999, in the UK) if the child or young person is at immediate risk

- Consider the risks to and the vulnerability of the pupil(s) involved, including carrying out checks with other agencies
- Inform parents and carers, where appropriate, about how the incident is being managed
- Make a referral to the relevant Children's Social Services and/or the Police
- Provide the necessary support for pupils, including counselling and pastoral support
- Review the handling of the incident, ensuring that any changes are implemented effectively to maintain best practice

We will respond to concerns regarding child sexual abuse and exploitation, regardless of whether the incident took place on school platforms or personal equipment.

Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: [www.ceop.police.uk/safety-centre/](http://www.ceop.police.uk/safety-centre/). There is also a CEOP button in the pupil common room that links to this website.

If we are unclear whether a criminal offence has been committed, the DSL/CPO will obtain advice immediately through the Police.

#### **d. Indecent Images of Children (IIOC)**

HeadG Online School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on the school platforms or on pupil personal devices.

We will seek to prevent accidental access to IIOC by ensuring teachers check all websites and platforms they are using, beforehand, when they are outwith Adobe and ~ Canvas. Parents and carers are strongly recommended to ensure that age appropriate websites are accessed in the home and that the necessary filtering and monitoring is taking place. As pupils school from home, the school has a limited ability to prevent pupils accessing this content accidentally.

If the school is unclear if a criminal offence has been committed, the DSL/CPO will obtain advice immediately from the Police.

If the school are made aware of IIOC, we will:

- Act in accordance with the relevant school policies i.e. safeguarding
- Immediately inform the appropriate external bodies and the police

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL/CPO is informed
- Ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk)
- Ensure that any copies that exist of the image, for example in emails, are deleted
- Report concerns, as appropriate to parents/carers

If made aware that indecent images of children have been found on the school platforms, we will:

- Ensure that the DSL/CPO is informed
- Ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk)
- Inform the Police (via 101 or 999, in the UK) where child is thought to be at immediate risk
- ensure that any copies that exist of the image, for example in emails, are deleted
- only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only
- report concerns, as appropriate to parents/carers

If made aware that a member of staff is in possession of indecent images of children on school platforms, we will:

- Ensure our DSL/CPO, Head of School and Director are informed and decisions will be made on how to proceed with such an allegation
- Block access to school platforms for the member of staff in question
- Contact the Police to seek advice on how to proceed

**e. Cyberbullying**

Cyberbullying, along with all other forms of bullying, will not be tolerated at the school. Full details of how we will respond to cyberbullying are set out in our anti-bullying and safeguarding policies

**f. Online Hate**

Online hate content, directed towards or posted by, specific members of the HeadG online School community will not be tolerated at the school and will be responded to in line with existing policies, including anti-bullying

and behaviour. All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL/CPO will obtain advice from the police.

#### **g. Online Radicalisation and Extremism**

We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing our school platforms. Parents and carers are strongly recommended to ensure that age appropriate websites are accessed in the home and that the necessary filtering and monitoring is taking place. As pupils school from home, the school has a limited ability to prevent pupils accessing extremist material that may seek to radicalise pupils.

If we are concerned that a child, young person or parent/carer may be at risk of radicalisation online, the DSL/CPO will be informed immediately, and action will be taken in line with the relevant policies i.e. safeguarding policies.

If we are concerned that members of staff may be at risk of radicalisation online, the DSL/CPO the Head of School and the Director will be informed immediately, and action will be taken in line with national guidance ([The Prevent Duty](#)) and any advice sought from the police.



## e-Safety Links

Link	Description
<a href="#">CEOP: Thinkuknow</a>	Suggested sites and internet safety advice by age group
<a href="#">ChildLine: Staying safe online</a>	ChildLine is a private and confidential service for children and young people up to the age of 19.
<a href="#">Childnet International: Parents and Carers</a>	Working to help make the internet a great and safe place for children.
<a href="#">Digital Trends: Android App Security Basics: Easy Ways To Keep Your Phone Safe</a>	How to avoid inadvertently downloading malware, basic tips to keep your Android phone safe and secure.
<a href="#">Digizen Family Agreement</a>	A common understanding of what is and what isn't appropriate behaviour online.
<a href="#">Internet Watch Foundation</a>	Report criminal online content securely and confidentially.
<a href="#">K9 Web Protection</a>	Free, enterprise-class security software designed for home computers
<a href="#">Kids Privacy: Tips &amp; Scripts for Parenting in the Digital World</a>	Information and resources for parents on raising kids in a digital world.
<a href="#">KidSMART</a>	SMART rules – (S)afe (M)eeting (A)ccepting (R)eliable (T)ell
<a href="#">Macworld: Set up a kid-friendly iPad</a>	Before handing over your iPad to a child, it's best to do some parental preparation.
<a href="#">National Crime Agency - Child Exploitation and Online Protection (CEOP)</a>	CEOP helps children stay safe online. Report inappropriate online behaviour.
<a href="#">NSPCC: Online porn</a>	Advice on how to talk to your child about the risks of online porn and sexually explicit material.
<a href="#">Virtual Global Taskforce</a>	An international partnership of law enforcement agencies, non-government organisations and industry to help protect children from online child abuse.
<a href="#">Xbox 360: Online safety and privacy settings</a>	Change the online safety and privacy settings for any profile on the Xbox 360 console
<a href="#">Xbox One: Family SecurityONE security</a>	Learn how to configure privacy and online safety settings for Xbox One.

**- END OF POLICY -**

