The Heath School

Heath MAT Online Safety Policy

October 2021-22

Key School Details

Designated Safeguarding Lead (s): (Helen Newcombe - Assistant Principal)

Named Governor with lead responsibility: (Jane Ainsworth- Chair of Governors)

Date written: October 2021

Date agreed and ratified by The Trust Board: October 2021

Date of next review: October 2022

This policy will be reviewed at least annually.

The online safety policy is recognised as a safeguarding policy, not a technical or computing policy and falls within the role and responsibilities the Designated Safeguarding Lead (DSL).

Contents

The Heath School Online Safety Policy

1. Policy Aims

- This online safety policy has been written by the schools Designated Safeguarding Lead along with the MAT Safeguarding Lead.

- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2021, Early Years and Foundation Stage 2021, 'Working Together to Safeguard Children' 2018 and the Halton Safeguarding Partnership procedures. Guidance for Safer working Practice for those working with children and young people in education Settings May 2019

- It takes into account the DFE 'teaching online safety in schools guidance, June 2019

- The purpose of *The Heath School* online safety policy is to:
    - Safeguard and protect all members of *The Heath School* community online.
    - Identify approaches to educate and raise awareness of online 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 online safety concerns.

- *The Heath School* identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

    - **Content:** being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

    - **Contact:** being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying

    - **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

- *The Heath School* will aim to:
  - Create a culture that incorporates the principles online safety across all elements of school life.
  - Proactively engage staff, students and parents/carers.
  - Build a partnership approach to online safety and will support parents/carers to become aware and alert to online safety issues.
  - Review, maintain and embed online safety principles.
  - Model online safety principles consistently.

2. Policy Scope

- *The Heath School* recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- All School owned devices and systems will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- *The Heath School* recognises the specific risks that can be posed by mobile technology, including mobile phones and cameras. In accordance with KCSIE 2021 has appropriate policies in place that are shared and understood by all members of the community.
- *The Heath School* will do all we reasonably can to limit children's exposure to online risks through our school/college IT systems
- *The Heath School* identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- *The Heath School* will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with School issued devices for use, both on and off-site.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
  - Anti-bullying policy
  - Acceptable Use Policies (AUP)
  - Code of conduct/staff behaviour policy

- Behaviour and discipline policy
- Confidentiality
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Relationships and Sex Education (RSE)
- Data security
- Cameras and image use
- Mobile phone and social media policies related policies or protocols
- Safeguarding/Child protection policy
- Searching, screening and confiscation

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. *The Heath School* along with the Heath Family will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any safeguarding/child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Principal/DSL will be informed of online safety concerns, as appropriate.
- The DSL will report on a regular basis to the governing body on online safety practice and incidents, including outcomes
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (*Helen Newcombe – Assistant Principal*) has lead responsibility for online safety and the safeguarding deputies hold delegated responsibility. Other staff and designated safeguarding staff have responsibility to respond to online safety concerns.
- *The Heath School* recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The Governors will:

- Review and formally receive the online safety policy and review its effectiveness. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.
- Meet regularly with the DSL and others responsible for online safety.

4.2 The leadership team will:

- Ensure the safety (including online safety) of members of the school community as the Principal holds the duty of care.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy *and* acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole school curriculum which enables all learners to develop an appropriate understanding of online safety.
- When implementing appropriate filtering and monitoring, *The Heath School* will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

4.3 The Designated Safeguarding Lead (DSL), or Designated Deputy will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the schools safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.

- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Respond to online safety concerns in line with the safeguarding/child protection and other associated policies such as anti-bullying and behaviour.
    - Internal sanctions and/or support will be implemented as appropriate.
    - Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the leadership team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with lead responsibility for safeguarding/online safety.

4.4 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies, where appropriate.
- Read and adhere to the online safety policy and acceptable use policies.
- 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 personal use of technology, both on and off site.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the schools safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.5 It is the responsibility of staff managing the technical environment to:

- Ensure that school meets required online safety technical requirements and any *Local* Authority/MAT/other relevant body online safety policy/guidance that may apply.
- Ensure that users may only access the networks and devices through a properly enforced password protection policy.
- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate related online safety policies and procedures.
- Implement appropriate security measures including: esafe, smoothwall, as directed by the leadership team to ensure that the schools IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.6 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies, where appropriate.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.7 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement *and/or* acceptable use policies.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies, where appropriate.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies that their children use at home.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- The school will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst learners by:
    - ensuring our curriculum and whole school approach is developed in line with KCSiE 2021, the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
    - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study.
    - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
    - implementing appropriate peer education approaches.
    - creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving the DSL (or a deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.
    - making informed decisions to ensure that any educational resources used are appropriate for our learners.
    - using external visitors, where appropriate, to complement and support our internal online safety education approaches (When reviewing online safety provision, the UKCIS external visitors guidance highlights a range of resources which can support educational settings to develop a whole school approach towards online safety.)
    - providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
    - rewarding positive use of technology.

- The school will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
    - Displaying acceptable use posters in all rooms with internet access.
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology where appropriate.
    - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- *The Heath School* will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
    - ensuring age appropriate education regarding safe and responsible use precedes internet access.

- teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
- educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
- enabling them to understand what acceptable and unacceptable online behaviour looks like.
- preparing them to identify possible online risks and make informed decisions about how to act and respond.
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Learners

- *The Heath School* recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- *The Heath School* will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
- Staff at *The Heath School* will seek input from specialist staff as appropriate, including the DSL, SENCO, Child in Care Designated Teacher to ensure that the policy and curriculum is appropriate to our community's needs.

.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.

- Make staff aware that their online conduct outside of the school, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- *The Heath School* recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- *The Heath School* recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the school is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

School will consider the following points and keep records as appropriate:

School owned/provided devices:

- *Who they will be allocated to*
- *Where, when and how their use is allowed – times/places/in school/out of school*
- *If personal use is allowed*
- *Levels of access to networks/internet (as above)*
- *Management of devices/installation of apps/changing of settings/monitoring*
- *Network/broadband capacity*
- *Technical support*
- *Filtering of devices*
- *Access to cloud services*
- *Data Protection*
- *Taking/storage/use of images*
- *Exit processes – what happens to devices/software/apps/stored data if user leaves the school*
- *Liability for damage*
- *Staff training*

Personal devices:

- *Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors)*
- *Restrictions on where, when and how they may be used in school*
- *Storage*
- *Whether staff will be allowed to use personal devices for school business*
- *Levels of access to networks/internet (as above)*
- *Network/broadband capacity*
- *Technical support (this may be a clear statement that no technical support is available)*
- *Filtering of the internet connection to these devices*
- *Data Protection*
- *The right to take, examine and search users devices in the case of misuse (England only)*
- *Taking/storage/use of images*
- *Liability for loss/damage or malfunction following access to the network*
- *Identification/labelling of personal devices*
- *How visitors will be informed about school requirements*
- *How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.*

7.1 Classroom Use

- *The Heath School* uses a wide range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites

    - Learning platform/intranet
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. They will use *tools SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search*.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
    - **Key Stage 3, 4**
        - Learners will be appropriately supervised when using technology, according to their ability and understanding.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- *The Heath School* governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Appropriate filtering

- *The Heath School* 's education broadband connectivity is provided through *BT*
- *The Heath School* uses *Smoothwall monitoring*
    - *Smoothwall* blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
    - *Smoothwall* is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
    - *Smoothwall* integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- We work with *Smoothwall* to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to report it to the Principal / Head Teacher

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
  The Heath uses Smoothwall for our firewall. This also monitors internet usage, and we also use Smoothwall filtering that actively monitors anything typed into the computer.

- If a concern is identified via monitoring approaches we will:
    - All concerns identified go straight to Safeguarding Online Safety coordinator, to the DSL and IT Lead Technician
    - SG online coordinator evaluates concern and either refers to pastoral or SG dependent on the nature of the incident
    - Incident recorded on CPOMS
    - Behaviour – pastoral/academic would be dealt with by either PC or HOD and behaviour sanctions put in place
    - SG – nature of comment evaluated
    - Students spoken to by member of SG team following SG policy/procedures and appropriate action taken
    - Incident recorded in CPOMS

- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

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

- Full information can be found in our trust Data Protection (GDPR) policy.

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on our network,
  - The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for all
  - All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 7, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

7.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our school address, email and telephone number.
- The administrator account for our 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.

7.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: Safeguarding and Child protection policy, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - School email addresses and other official contact details will not be used for school or personal social media accounts.
- Members of the community will immediately tell the principal or DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted.

7.8.1 Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- Similarly, school/trust provided email addresses are not permitted to be used for personal communications.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

7.8.2 Learner email

- Learners will use provided email accounts for educational purposes.
- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Videoconferencing and/or Webcams

- *The Heath School* recognise that videoconferencing *and/or* use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing *and* webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.

- Videoconferencing contact details will not be posted publically.
- Videoconferencing equipment will not be taken off the premises without prior permission from the Principal/Head of School
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

7.10 Management of Learning Platforms

- *The Heath School* uses (*ClassCharts*) as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff *and/or* learners leave the school, their account will be disabled or transferred to their new establishment.

- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.

- Any concerns about content on the LP will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
  - Access to the LP for the user may be suspended.
  - The user will need to discuss the issues with a member of leadership before reinstatement.
  - A learner's parents/carers may be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures/behaviour policy or staff code of conduct.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.11 Management of Applications (apps) used to Record Children's Progress

- We use **Sisra and Sims** to track learners progress and share appropriate information with parents and carers.
- The *Principal* is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
  - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
  - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
  - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

7.12 Where children are asked to learn online at home in response to a full or partial closure:

- *The Heath School* will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.

- All communication with learners and parents/carers will take place using school/college provided or approved communication channels; for example, school provided email accounts and phone numbers and/or agreed systems e.g. Teams, Google Classroom, Microsoft 365 or equivalent
- Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our school behaviour policy/code of conduct and Acceptable Use Policies.
- Staff and learners will be encouraged to report issues experienced at home and concerns will be responded to in line with our safeguarding/child protection and other relevant policies.
- When delivering remote learning, staff will follow our Acceptable Use Policy (AUP).
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. *The Heath School* will continue to be clear who from the school (if anyone) their child is going to be interacting with online.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.
- Additional guidance for DSLs and SLT regarding remote learning is available at DfE: 'Safeguarding in schools colleges and other providers' and 'safeguarding and remote education'. Advice is also available from NSPCC and PSHE Association also provide helpful advice:
    - NSPCC Learning - Undertaking remote teaching safely during school closures
    - PSHE - PSHE Association coronavirus hub
- Where a class, group or small number of pupils need to self-isolate, or there are local restrictions requiring pupils to remain at home, the Department for Education expects schools to be able to immediately offer them access to remote education. *The Heath School* will, where possible, ensure remote education, where needed, is safe, high quality and aligns as closely as possible with in-school provision.
- *The Heath School* will continue to improve the quality of remote education and have a strong contingency plan in place for remote provision.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of *The Heath School* community.
- 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.
- If using social media, all members of *The Heath School* community are expected to engage in a positive, safe, appropriate and responsible manner. In line with this all members of *The Heath School* community are advised to carefully consider what they publish on social media, specifically regarding detailed private thoughts, concerns, pictures or messages especially content that may be considered threatening, hurtful or defamatory to others.

- We will control learner and staff access to social media whilst using school provided devices and systems on site.
    - The use of social media during school hours for personal use *is not* permitted for staff.
    - The use of social media during school hours for personal use *is not* permitted for learners.
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- The use of social media or apps as a formal remote learning platform following Covid-19 restrictions will be robustly risk assessed by SLT prior to use by staff or learners. The use of such platforms will only take place in accordance with out our acceptable use policy.
- Concerns regarding the online conduct of any member of *The Heath School* community on social media, should be reported to the DSL/Principal, as appropriate and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Staff Personal Use of Social Media

- 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 via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

8.2.1 Reputation

- 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.
    - Civil, legal or disciplinary action may be taken if staff 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 sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (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.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of *The Heath School* on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to 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 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 learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Principal/DSL immediately if they consider that any content shared on social media sites conflicts with their role.

8.2.2 Users Communicating with learners and parents and carers

- Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.
- All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the Principal.
    - Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the school and members of staff.
- If ongoing contact with learners is required once they have left the school, members of staff will be expected to use existing alumni networks, or use official school provided communication tools.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy) *and/or* the Principal.

8.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
    - 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 safe passwords.

- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the school and externally.

8.4 Official Use of Social Media

- *The Heath School* official social media channels are:
  - *List details e.g. Twitter link:* @TheHeathSchool
- The official use of social media sites only takes place with clear educational or community engagement objectives and with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the *Principal*
  - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
  - Staff use school provided email addresses to register for and manage official social media channels.
  - Official social media sites are suitably protected and, where possible, run *and/or* linked *to/from* our website.
  - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the school will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving learners will be moderated if possible.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- 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.

8.4.1 Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals 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:
  - Sign our social media acceptable use policy.

- Be aware they are an ambassador for the school.
- Be professional, 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 libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure appropriate consent has been given before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so.
- Not engage with any private/direct messaging with current or past learners or parents/carers.
- Inform their line manager, the DSL (or deputy) and/or the Principal of any concerns, such as criticism, inappropriate content or contact from learners.

9. Mobile Technology: Use of Personal Devices and Mobile Phones

- *The Heath School* recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the school.

9.1 Expectations

- All use of mobile technology including personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour, child protection and Staff code of conduct.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
  - All members of our school community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - All members of our school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our anti bullying and behaviour policies.
- All members of our school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Staff providing formal remote learning because of Covid-19 restrictions or for other specified reasons, will do so using school/setting provided equipment in accordance with our acceptable use policy.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time.
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson and contact times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written permission has been given by the *Principal*, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the DSL or Principal.
- Staff will not use personal devices:
    - To take photos or videos of learners and will only use work-provided equipment for this purpose.
    - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Learners Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
    - *The Heath School* expects learners' personal devices and mobile phones to be***, switched off, kept out of sight during lessons and while moving between lessons.***
- If a learner needs to contact his/her parents or carers they will be allowed to use a *school* phone ***e.g. the office phone.***

- Parents are advised to contact their child via the *school* office;
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time
    - If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
- Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- Where learners' mobile phones or personal devices are used when learning at home, such as in response to local or full lockdowns, this will be in accordance with our Acceptable Use Policy.
- If a learner breaches the policy, the phone or device will be confiscated and held in a secure place.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
    - Searches of mobile phone or personal devices will be carried out in accordance with our policy. In line with the DfE '***Searching, Screening and Confiscation'*** guidance.
    - Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
    - Mobile phones and devices that have been confiscated will be released to students/ parents/ carers at the end of the day on Friday of each week.
    - If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) should ensure that they:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time.
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson and contact times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written permission has been given by the *Principal*, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations

- Appropriate signage and information is provided to inform parents, carers and visitors of expectations of use.
- Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL or Principal of any breaches our policy.

9.5 Officially provided mobile phones and devices **(If provided)**

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.
- Staff providing formal remote learning because of Covid-19 restrictions, will do so using school/setting provided equipment in accordance with our acceptable use policy.

10. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Service.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Service or Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Principal will speak with the Police *and/or* the Education Safeguarding Service first to ensure that potential investigations are not compromised.

10.1 Concerns about learner online behaviour and/or welfare

- The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
- All concerns about learners will be recorded in line with our child protection policy.
- School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the Principal, in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff *behaviour policy/code of conduct*.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Principal and/or DSL (or deputy). The Principal and/or DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11. Procedures for Responding to Specific Online Concerns

11.1 Online sexual violence and sexual harassment between children

- Our Principal, DSL and appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2021) guidance and part 5 of 'Keeping children safe in education' 2021.
    - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
- School recognises that sexual violence and sexual harassment between children can take place online. Examples may include;
    - Non-consensual sharing of sexual images and videos
    - Sexualised online bullying

  - Online coercion and threats
  - 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
  - Unwanted sexual comments and messages on social media
  - Online sexual exploitation
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
  - immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
  - if content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
  - implement appropriate sanctions in accordance with our behaviour policy.
  - inform parents and carers, if appropriate, about the incident and how it is being managed.
  - if appropriate, make referrals to partner agencies, such as Children's Social Work Service and/or the police.
  - if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police 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.
- School recognises that 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.
- School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

11.2 Youth produced sexual imagery ("sexting")

- School recognises youth produced sexual imagery (also known as "sexting" or 'consensual sharing or non-consensual sharing of nudes and semi-nude images') as a safeguarding issue and may be a sign that a child is at risk; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and the local guidance:
    - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery 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 the taking and sharing of youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using school provided or personal equipment.
- We will not:
    - view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
        - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - act in accordance with our safeguarding and child protection policies and the relevant local procedures.
    - ensure the DSL (or deputy) responds in line with the UKCIS.
    - store any devices containing potential youth produced sexual imagery securely
        - If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.

- make a referral to Children's Social Work Service and/or the police, as deemed appropriate in line with the UKCIS and guidance.
- provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the UKCIS guidance.
    - Images will only be deleted once the DSL 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 any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.
- School will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community and can be accessed readily from the school website.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant procedures.
    - store any devices containing evidence securely.
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk.
    - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.

    - provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using school provided or personal equipment.
    - Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).
- If members of the public or learners at other schools are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant procedures.
    - store any devices involved securely.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via 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 and carers.
- If made aware that indecent images of children have been found on the school provided devices, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - 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 provided devices, we will:
    - ensure that the Principal is informed in line with our managing allegations against staff policy.
    - inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
    - quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at *The Heath School*
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.6 Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at school and will be responded to in line with existing policies, including child protection, 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 (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

11.7 Online radicalisation and extremism

- As listed in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.

- If we are concerned that member of staff may be at risk of radicalisation online, the Principal will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12. Useful Links

National Links and Resources for Schools, Learners and Parents/carers

The following list (taken from KCSiE 2021, Annex D) is not exhaustive but should provide a useful starting point:

Advice for governing body and senior leaders

• Childnet provide guidance for schools on cyberbullying

• Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation

• London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

• NSPCC provides advice on all aspects of a school or college's online safety arrangements

• Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective

• Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones

• South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

• Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

• UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring

• Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.

• Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to

protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

- Internet Watch Foundation (IWF): www.iwf.org.uk
- Action Fraud: www.actionfraud.police.uk

Remote education, virtual lessons and live streaming

• Case studies on remote education practice are available for schools to learn from each other

• Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely

• London Grid for Learning guidance, including platform specific advice

• National cyber security centre guidance on choosing, configuring and deploying video conferencing

• National cyber security centre guidance on how to set up and use video conferencing

• UK Safer Internet Centre (UKCIS) guidance on safe remote learning

Support for children

• Childline for free and confidential advice

• UK Safer Internet Centre to report and remove harmful online content

• CEOP for advice on making a report about online abuse

Parental support

• Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support

• Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents

• Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

• Government advice about security and privacy settings, blocking unsuitable content, and parental controls

• Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world

• Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation

• London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

• Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

• National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

• Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games

• Parentzone provides help for parents and carers on how to keep their children safe online

• Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations

• UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Annex 1 - Responding to an Online Safety Concern Flowchart