| Status | Approved & Adopted | Approval | Full Governing Body |
|---|---|---|---|
| Maintenance | Full Governing Body | Role(s) responsible | Head Teacher |
| Date Effective | 21 June 2021 | Date of last review | June 2021 |
| Date of next review | June 2023 | Date withdrawn | Not withdrawn. |
| Lead Professional | Deputy Headteacher | Location of policy | www.coltonhills.co.uk |

## COLTON HILLS COMMUNITY SCHOOL

**Rationale**

The purpose of Colton Hills Community School online safety policy is to:

Safeguard and protect all members of Colton Hills Community 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

## CONTENTS

**Disclaimer**

The template has been created by the Education People. The Education People make every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable.

The copyright of these materials is held by The Education People. However, educational settings that work with children and young people are granted permission to use all or part of the materials for not-for-profit use, providing the Education People copyright is acknowledged and we are informed of its use.

**This policy will be reviewed <u>at least</u> annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure**

## 1. Policy Aims

- This online safety policy has been written by Colton Hills Community School.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2020, and the Wolverhampton Safeguarding Partnership Board procedures.

- The purpose of Colton Hills Community School online safety policy is to:
  - o Safeguard and protect all members of Colton Hills Community School community online.
  - o Identify approaches to educate and raise awareness of online safety throughout the community.
  - o Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  - o Identify clear procedures to use when responding to online safety concerns.

- Colton Hills Community School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
  - o **Content:** being exposed to illegal, inappropriate or harmful material
  - o **Contact:** being subjected to harmful online interaction with other users
  - o **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

## 2. Policy Scope

- Colton Hills Community School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online.
- Colton Hills Community School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Colton Hills Community School believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as students, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

### 2.2 Links with other policies and practices

- o This policy links with several other policies (but not limited to):
- o Anti-bullying policy
- o Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
- o Behaviour policy
- o Safeguarding and Child protection policy

o Curriculum policies, such as: (PSHE), Citizenship and Relationships and Sex Education (RSE)

## 3. Monitoring and Review

- Technology in this area evolves and changes rapidly; Colton Hills Community School will review this policy at least annually
  - o The policy will also be revised following any national or local policy requirements, any 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 DSL, ICT, and safeguarding team will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding (Manju Raillay and Sutinder Herian) will report on a regular basis to the governing body on online safety practice and incidents, including outcomes, which will come from Governor Link Meetings with the DSL.
- Any issues identified via monitoring will be incorporated into our action planning.

## 4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Tom Hazell has lead responsibility for online safety.
  - o Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.
- Colton Hills Community School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

## 4.1 The leadership and management team will:

- 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; as schools increasingly work online, it is essential that children are safe guarded from potentially harmful and inappropriate online material (including when they are online at home).
- Ensure that online safety is embedded within a progressive curriculum, which enables all students 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.

## 4.2 The Designated Safeguarding Lead (DSL) 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 settings 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 students safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that students 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.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings 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 SLT and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually).
- Meet regularly with the link governor(s) with a lead responsibility for safeguarding *and/or* online safety.

## 4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting 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.
- 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 settings 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.

**4.4 It is the responsibility of staff managing the technical environment to:**

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures to ensure that the settings 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 is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL (or deputy DSLs) and leadership team, as well as, the settings Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

**4.5 It is the responsibility of students (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.
- 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.

**4.6 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.
- Abide by the acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- 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.

**5.    Education and Engagement Approaches**

**5.1 Education and engagement with students**

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst students by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Relationship, Social, Health and Economic (RSHE), Relationships and Sex Education (RSE) and computing programmes of study.  Online safety is also to be covered in each year of the KS3 IT/ Computing curriculum.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Colton Hills Community School will support students 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 students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology.
  - Implementing appropriate peer education approaches.
  - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
  - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

## 5.2 Vulnerable Students

- Colton Hills Community School recognises that some students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Colton Hills Community School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.
- When implementing an appropriate online safety policy and curriculum Colton Hills Community School will seek input from specialist staff as appropriate, including the SENCO, Designated Teacher for CiC and other appropriate staff.

## 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 be done through stand-alone sessions or through drip feeding with small sessions/ daily bulletin reminders. Colton Hills Community also have a subscription to the

National College for online training support for staff who will be directed towards online safety training.

- o This will cover the potential risks posed to students (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 setting, 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 students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the community.

## 5.4 Awareness and engagement with parents and carers

- Colton Hills Community 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:
- o 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 and transition events as well as on twitter. (Parent forum and online support package)
    - o Drawing their attention to the online safety policy and expectations on our website.
    - o Requesting that they read online safety information as part of joining our community.
    - o Requiring them to read our acceptable use policies and discuss the implications with their children.

## 6. Reducing Online Risks

- Colton Hills Community School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - o Regularly review the methods used to identify, assess and minimise online risks.
    - o Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - o Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - o 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

### 7.1 Classroom Use

- Colton Hills Community School uses a wide range of technology. This includes access to:
    - o Computers, laptops and other digital devices
    - o Internet which may include search engines and educational websites
    - o Email
    - o 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 always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting 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 students complies with copyright law and acknowledge the source of information.
- Supervision of students will be appropriate to their age and ability.

### 7.2 Managing Internet Access
- We will maintain a record of users who are granted access to our devices and systems.
- All staff, students 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
- Colton Hills Community School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit student'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 process 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 students; effective classroom management and regular education about safe and responsible use is essential.

### 7.3.2 Filtering

- Education broadband connectivity is provided through the local authority.
- We use the local authority's Lightspeed filtering system, which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
- We work with the local authority to ensure that our filtering process is continually reviewed.
- If students discover unsuitable sites, they will be required to:
  - **Turn off monitor/screen and report the concern immediate to a member of staff.**
  - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputies) and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, West Midlands Police or CEOP.

### 7.3.4 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - Use of our monitoring systems such as Lightspeed. Reports are sent to the Safeguarding team to investigate
- If a concern is identified via monitoring approaches we will:
  - Log a concern and the Safeguarding team will respond in line with the child protection policy.
- 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.

### 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.
  - 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.
- All students are provided with their own unique username and private passwords to access our systems; students are responsible for keeping their password private.
- We require all users to:
    - o Use strong passwords for access into our system.
    - o Change their passwords twice a year
    - o Always keep their password private; users must not share it with others or leave it where others can find it.
    - o 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 student'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: data security, acceptable use policies, codes of conduct/behaviour.

### 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.
    - o The forwarding of any chain messages/emails is not permitted.
    - o Spam or junk mail will be blocked and reported to the email provider.
    - o Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - o Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

 Members of the community will immediately inform the 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; access to external personal email accounts may be blocked on site.
 Any concerns can be logged via our safeguarding software My Concern. The Safeguarding team can be contacted via chcssafeguarding@coltonhills.co.uk

### 7.8.1 Staff email

 The use of personal email addresses by staff for any official setting business is not permitted.
   o All members of 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, students and parents.

### 7.8.2 Student email

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

### 7.9 Live Stream Lessons for Remote Learning

 Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another.  In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves.  In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function.

 When planning the use of live stream platforms within remote learning our school will:
   o Consider whether the technology is available to children/families and make alternative arrangements for provision where necessary.
   o Ensure that staff are trained to use the technology.
   o Ensure that children's behaviour/interactions are managed in line with the expectations of the school behaviour policy.
   o Risk assess the platform being used and consider whether there are functions, such as live chat, pupil's use of video camera, or the recording of the session, which need to be disabled or which require further measures to support their appropriate use.

The above points are relevant to live stream in its broadest sense.  What follows next is more relevant, but not exclusively, to the use of platforms allowing two-way video interaction between all users.

 Where possible two members of staff will be 'within the room' when conducting a live stream session with pupils.  If the session is being run from school and both adults are there, then they can be physically within the same room.  If one or both adults are working remotely then this means that two adults will need to be present within the video call, and they should both be there before the pupils dial in.
 The second member of staff is there to provide a safeguard for both the pupils and the teacher, so

does not need to be a curriculum specialist. Where a second member of staff is not available then the session is recorded.

- The second member of staff could act additionally as technical/behaviour support, in terms of monitoring pupils' interactions and ensuring they are not using chat or recording features if these cannot be disabled.
- Sessions will be planned and scheduled for during school hours.
- Parents will be contacted to advise that the session is taking place and they and the child should consent to abide to an acceptable use agreement covering issues such as not recording the session, not using the live chat feature, being appropriately dressed etc.
- Only school devices and school contact numbers/emails will be used for communications and running the session.
- Only live streaming platforms approved by SLT will be used.
- Staff will dress professionally and choose a neutral background for their video stream.
- Students should be dressed appropriately e.g. clothes they might wear for a non-uniform day, not pyjamas.
- Students should live stream from a suitable location within their household, not bedrooms.
- Staff behaviour and language will be entirely in line with the staff code of conduct.
- All other school policies/practices should be followed, notably the safeguarding and child protection policy so should there be any welfare concerns about the child these should be brought to the attention of the DSL without delay.

**Live Stream from other providers**

- When directing students to any content from other providers, its suitability and appropriateness will be checked.
- Where that content may be live streamed, the safeguarding aspect of how that content is being delivered will be considered e.g. how children are able to interact, how is content and interactions being monitored/moderated etc?
- For one off live stream events, the content will be monitored by a member of staff along with the interactions/behaviour of the students taking part.
- When/if multiple sessions are being run at various times during the school day, school leaders will check that they are satisfied with the safeguarding policy of the provider(s) and, then, monitor some sessions to check they are in accordance with the policy.

**Using video calls for 1:1 sessions with children**

- The school may consider using 1:1 video call sessions to support interventions with children such as mental health support or counselling.
- These sessions will only be provided where they have been risk assessed and approved by SLT.
- Where the communication with an individual child does not require the confidentiality of a counselling session, ideally there will be two adults involved; this will provide a safeguard for the adults and the children.
- These two adults will either be physically in the same room, with the second member of staff being referenced to the child so that they are aware, or, where staff are working remotely, they will both be within the virtual room of the meeting.
- In either case both adults will be present before the child is admitted to the online session.
- If this is not possible due to counselling etc then parents must be made aware of the session and if the meeting is not confidential then it should be recorded.

## 7.10 Management of Learning Platforms

- 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, students and parents will have access to the LP.
- When staff and/or students leave the setting, their account will be disabled or transferred to their new establishment.
- Students 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 student's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.
- Students may require editorial approval from a member of staff. This may be given to the student 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 SIMS and Go4Schools to track students progress and share appropriate information with parents and carers.
- The headteacher 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 student's data:
    - Only student issued devices will be used for apps that record and store students' 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 students' 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.

## 8. Social Media

## 8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Colton Hills Community 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 Colton Hills Community School are expected to engage in social media in a positive, safe and responsible manner.
  - o All members of Colton Hills Community School 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.
- We will control student and staff access to social media whilst using setting provided devices and systems on site.
  - o The use of social media during setting hours for personal use is not permitted.
  - o Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Colton Hills Community School community on social media, should be reported to the DSL (or deputy) or Headteacher 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.

*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 setting.
  - o 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):
  - o Setting the privacy levels of their personal sites.
  - o Being aware of location sharing services.
  - o Opting out of public listings on social networking sites.
  - o Logging out of accounts after use.
  - o Keeping passwords safe and confidential.
  - o 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 Colton Hills Community

School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, 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 students and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

*Communicating with students and parents and carers*

- All members of staff are advised not to communicate with or add as 'friends' any current or past students or their family members via any personal social media sites, applications or profiles.
  o Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the headteacher.
  o If ongoing contact with students is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher/line manager.
- Any communication from students and parents received on personal social media accounts will be reported to the DSL (or deputies).

**8.3 Students Personal Use of Social Media**

- Safe and appropriate use of social media will be taught to students 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 students under this age.

- Any concerns regarding students use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
  o Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Students will be advised:
  o To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
  o To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
  o Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
  o To use safe passwords.

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

## 8.4 Official Use of Social Media

Colton Hills Community School official social media channels are a twitter account Colton Hills CS @ColtonHillsCS:

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - o The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
    - o 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 social media sites or accounts for educational or engagement purposes only.
    - o Staff use setting provided email addresses to register for and manage any official social media channels.
    - o Official social media sites are suitably protected and linked to our website.
    - o Public communications on behalf of the setting 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: anti- bullying, data protection, code of conduct, and child protection.
    - o All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - o Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - o Any official social media activity involving students will be moderated if possible.
- Parents and carers will be informed of any official social media use with students; 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.

*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 setting, they will:
    - o Sign our acceptable use policy.
    - o Always be professional and aware they are an ambassador for the setting.
    - o Disclose their official role but make it clear that they do not necessarily speak on behalf

of the setting.

o Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.

o Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.

o Ensure that they have appropriate consent before sharing images on the official social media channel.

o Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.

o Not engage with any direct or private messaging with current, or past, students, parents and carers.

o Inform their line manager, the DSL (or deputies) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from students.

## 9. Use of Personal Devices and Mobile Phones

 Colton Hills Community School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the school.

### 9.1 Expectations

 All use of 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 and child protection.

 Electronic devices of any kind that are brought onto site are the responsibility of the user.

o All members of Colton Hills Community 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.

o All members of Colton Hills Community 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 and student toilets.

 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 behaviour policy.

 All members of Colton Hills Community School 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 will be advised to:
  - o Keep mobile phones and personal devices in a safe and secure place during lesson time.
  - o Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - o Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  - o 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 pupils or parents and carers. Unless permission is sought with exceptional circumstances and the staff number hidden.
  - o Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies) and/or headteacher.
- Staff will not use personal devices:
  - o To take photos or videos of students and will only use work-provided equipment for this purpose.
  - o Directly with students and will only use work-provided equipment during lessons or 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
  - o 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 Students Use of Personal Devices and Mobile Phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Colton Hills Community School expects students' personal devices and mobile phones to be switched off and out of sight during the school day.
- If a student needs to contact his/her parents or carers they will be allowed to use a school phone or use their own mobile during break and lunch only.
  - o Parents are advised to contact their child via the school's main reception; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.
- Mobile phones or personal devices will not be used by students during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
  - o The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
  - o If members of staff have an educational reason to allow students to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Senior Leadership Team.

- Mobile phones and personal devices must not be taken into examinations.
    - o Students 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.
- If a student breaches the policy, the phone or device will be confiscated and will be held in a secure place.
    - o Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
    - o Searches of mobile phone or personal devices will only be carried out in accordance with our policy. www.gov.uk/government/publications/searching-screening-and- confiscation)
    - o Students mobile phones or devices may be searched by a member of the leadership team, with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. www.gov.uk/government/publications/searching-screening-and-confiscation)
    - o Mobile phones and devices that have been confiscated will be released to parents or carers.
    - o If there is suspicion that material on a student'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) must 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.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or headteacher of any breaches our policy.

## 9.5 Officially provided mobile phones and devices
- Senior members of staff will be issued with a work phone number and email address, where contact with students 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 associated policies, such as: anti-bullying, behaviour, child protection and image use.

## 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.

- o Students, 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 students 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.
- Safeguarding concerns and incidents should be reported to Wolverhampton MASH, in line with Wolverhampton Safeguarding and local authority Child Protection model policy.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the school safeguarding team.
- Where there is suspicion that illegal activity has taken place, we will contact the School safeguarding team, Wolverhampton MASH or West Midlands 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 headteacher will speak with West Midlands Police and/or the Wolverhampton MASH first to ensure that potential investigations are not compromised.

**10.1 Concerns about Students Welfare**

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.
  - o The DSL (or deputies) will record these issues in line with our child protection policy.
- The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Wolverhampton Safeguarding Partnership thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

**10.2 Staff Misuse**

- Any complaint about staff misuse will be referred to the headteacher, in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

**11. Procedures for Responding to Specific Online Incidents or Concerns**

**11.1 Online Sexual Violence and Sexual Harassment between Children**

- Our school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2020.

 Colton Hills Community 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, unwanted sexual comments and messages on social media, and online sexual exploitation.

  o Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

 Colton Hills Community 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.

 Colton Hills Community School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

 Colton Hills Community 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 between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSHE curriculum.

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

 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 online sexual violence and sexual harassment, we will:

  o Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

  o If content is contained on students electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

  o Provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.

   o Implement appropriate sanctions in accordance with our behaviour policy.

  o Inform parents and carers, if appropriate, about the incident and how it is being managed.

  o If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.

  o If the concern involves children and young people at a different educational setting, 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 West Midlands Police first to ensure that investigations are not compromised.

  o Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

## 11.2 Youth Produced Sexual Imagery ("Sexting")

 Colton Hills Community School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; 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 UKCCIS guidance: ' Sexting in schools a nd co lle ges: respo nd ing t o in cident s a nd saf eg uard ing youn g peo pl e' .

- Colton Hills Community 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. (including assemblies, PSHE programme and working with the local police liaison)
- 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/off site or using setting provided or personal equipment.
- We 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 (or deputy 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 students 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 child protection policies and the relevant Wolverhampton Safeguarding Partnership procedures.
  - Ensure the DSL (or deputy) responds in line with the ['Sexting in schools and colleges: respon di ng t o inci dent s an d saf eg uard ing you ng p eop le'](#) guidance.
  - Store the device securely.
    - ☐ If an 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 which considers any vulnerability of students involved; including carrying out relevant checks with other agencies.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to Children's Social Care and/or the Police, as appropriate.
  - Provide the necessary safeguards and support for students, 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 UKCCIS: ['Sexting in schools and col le ges: respo ndi ng t o inc ide nt s and saf e guar din g youn g pe opl e'](#) 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 Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Colton Hills Community 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.

- Colton Hills Community 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 (or deputy).
- 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 students, 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), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to students and other members of our community. This is available on the website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  - Act in accordance with our child protection policies and the relevant Wolverhampton Safeguarding Partnership procedures.
  - If appropriate, store any devices involved securely.
  - Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
  - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Provide the necessary safeguards and support for students, 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 child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
  - Where possible, students 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/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Wolverhampton MASH and/or Police.
- If students at other setting are believed to have been targeted, the DSL (or deputy) will seek support from the Police and/or Wolverhampton MASH first to ensure that potential investigations are not compromised.

**11.4 Indecent Images of Children (IIOC)**

- Colton Hills Community 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 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 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 Wolverhampton MASH.

- If made aware of IIOC, we will:
    - o Act in accordance with our child protection policy and the relevant Wolverhampton Safeguarding Partnership procedures.
    - o Store any devices involved securely.
    - o Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), West Midlands police or the LADO.

- If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:
    - o Ensure that the DSL (or deputy DSL) is informed.
    - o Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - o Ensure that any copies that exist of the image, for example in emails, are deleted.
    - o Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - o Ensure that the DSL (or deputy DSL) is informed.
    - o Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - o Ensure that any copies that exist of the image, for example in emails, are deleted.
    - o Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - o 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.
    - o Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - o Ensure that the headteacher is informed in line with our managing allegations against staff policy.
    - o Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
    - o 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 Colton Hills Community School
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy which is published on our website.

## 11.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Colton Hills Community 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 (or deputy DSL) will obtain advice through the Wolverhampton MASH and/or West Midlands Police.

## 11.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site. Internet use is monitored through the Lightspeed systems with daily reporting of risk categories to the safeguarding team.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) 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 headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

## 12. Useful Links for Educational Settings

**Wolverhampton Support and Guidance:**

- Wolverhampton Council Education Department
  www.wolverhampton.gov.uk/education-and-schools

- Wolverhampton Education Services
  https://wves.wolverhampton.gov.uk

- If you are concerned about a child in Wolverhampton contact Wolverhampton MASH on 01902 555392

- Local Authority Designated Officer:       Kenny Edgar        LADO@wolverhampton.gov.uk

**Wolverhampton Safeguarding Children's Partnership**

- 　www.wolverhamptonsafeguarding.org.uk
  https://westmidlands.procedures.org.uk

**West Midlands Police:**

www.west-midlands.police.uk

For non-urgent Police contact 101

If you think the child is in immediate danger, you should call the police on 999.

**National Links and Resources for Educational Settings**

- CEOP:
  - o www.thinkuknow.co.uk
  - owww.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - o ChildLine: www.childline.org.uk
  - o Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - o Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

**National Links and Resources for Parents/Carers**
- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - o www.thinkuknow.co.uk
  - o www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - o ChildLine: www.childline.org.uk
  - o Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

There is a wealth of information available to support schools and parents/carers to keep children safe online. See Keeping Children Safe in Education 2020 (Annex C) for more resources.