Online Safety Policy

DOCUMENT CONTROL	
Document Title: **Online Safety Policy**	
Version Number: **2023/1**	Author(s) name and job title: **Mrs H Larkin - Head of Safeguarding & Welfare**
Date Approved: **TBA**	Document status: **DRAFT**
Effective Date: **November 2023**	Approved by: **Local Advisory Board**
Superseded Version: **2022/3 (June 2022)**	Date of next review: **October2024**

1. Intent

This policy is to be read in conjunction with the latest Keeping Children Safe in Education guidance, as well as the FGS Safeguarding & Child Protection and Behaviour policies. Flixton Girls School understands that using online services is an important aspect of raising educational standards, promoting student achievement and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of students and staff.

Our school aims to

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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

Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, 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: 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 measures implemented to protect students and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

The Principal is responsible for:

- Ensuring that staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training
- Ensuring online safety practices are audited and evaluated
- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school

The DSL & Deputy DSLs:

Details of the school's designated safeguarding lead (DSL)and Deputy Designated Safeguarding Leads (DDSLs) are set out in our Safeguarding and Child Protection Policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal and governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT provider to make sure the appropriate systems and processes are in place
- Working with the Principal, ICT provider and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's Safeguarding policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or governing body
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

The ICT Provider:

The ICT Provider is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing how to report any incidents of those systems or processes failing by alerting the DSL or Principal
- Following the correct procedures by alerting the DSL if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of **'it could happen here'**

Parents / carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Students are responsible for:

- Adhering to this policy, the Acceptable Use Agreement and other relevant policies
- Seeking help from staff if they are concerned about something they or a peer have experienced online
- Reporting online safety incidents and concerns in line with the procedures within this policy.

4. The curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

· Health and Wellbeing

· PSHE

· Computing / Computer Science

See Appendix One for the school's approach to online Safety within the Curriculum

5. Staff training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

6. Educating Parents

The school works in partnership with parents to ensure students stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents can find a copy of the Acceptable Use Agreement in the student school planner, and they are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it. Ways of communicating this with parents is in Appendix Two, as are examples of risks posed.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group, by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also sends information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected. Literature is also available in school for parents / carers' use.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

If appropriate, the DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

The Principal, and any member of staff authorised to do so by the Principal, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the students co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff

member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / or Principal to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

7.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

FGS recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

FGS will treat any use of AI to bully students in line with our behaviour policy.

8. Classroom Use

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Chromebooks
- Tablets
- Intranet
- Google Workspace
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers also ensure that any internet-derived materials are used in line with copyright law. Students are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

9. Internet Access

Students, staff and other members of the school community are only granted access to the school's internet network once they have read and agreed to the Acceptable Use Agreement. Anyone using the school internet network is identifiable and agrees to the Acceptable Use Agreement. All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately. We will monitor the websites visited by students, staff, volunteers, governors and visitors to ensure they comply with the above and restrict access through filtering systems where appropriate.

10. School-Owned Devices

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the school / the ICT Provider.

11. Use of Personal Devices

Personal devices are used in accordance with the Acceptable Use Agreement, and are the responsibility of the user.

- Staff members are not permitted to use their personal devices during school hours, other than in an emergency, or for when accessing essential school-related or educational content and a school computer is unavailable
- If a staff member is using their device during free time in school, this should be out of view of students
- Staff members are not permitted to use their personal devices to take photos or videos of students, without express permission from the Principal
- Staff members are not permitted to store any school data on personal devices – any data downloaded or images taken must be deleted as soon as practical
- Personal devices are not permitted to be used in the toilets or changing rooms
- Students are not permitted to use their personal devices during school hours - if a student needs to contact their parents during the school day, they must go to a House Office for assistance.

12. Filtering and Monitoring Online Activity

The school ensures there are appropriate filters and monitoring systems in place; the filtering and monitoring systems we implement are appropriate to students' ages, and the risks posed online. The DSL / Deputy DSLs oversee checks on the filtering and monitoring systems. Reports of inappropriate use, websites or materials are investigated and the student spoken to. Reduced filtering can only be applied with the permission of the Principal / DSL.

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Where there is a concern that illegal activity has taken place, the school contacts the police and other relevant agencies. All online safety incidents and the school's response are recorded by the investigating staff on CPOMS.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Network Security

Technical security features, such as anti-virus software, are kept up-to-date and managed by our ICT provider. Firewalls are switched on at all times, and these are reviewed regularly to ensure they are running correctly, and to carry out any required updates. Staff and students are reminded not to download unapproved software or open unfamiliar email attachments.

Staff and students have their own unique usernames and private passwords to access the school's systems. Each person is responsible for keeping their passwords private. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. Users are required to lock access to devices and systems when they are unattended / unsupervised, or not in use. Staff are reminded and are trained about sharing sensitive details in emails, as well as the safe use of classroom projectors when students are in the room.

14. Responding to specific online safety concerns

Specific online safety concerns increase with the growth of online provision - Appendix Four details our procedures and response to - Cyberbullying, Online sexual violence and harrassment, Upskirting, Sexting and the Sharing of Indecent Imagery of Students, Online Abuse and Exploitation, Online Hate, Online Radicalisation and Extremism, and Online Hoaxes and Harmful Online Challenges.

15. Social networking -

The school's official social media channels are only used for official educational or engagement purposes, with named staff having access to update / amend posts. All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

See Appendix Three for guidance on personal social networking.

APPENDIX ONE - CURRICULUM INFORMATION FOR ONLINE SAFETY

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

Students are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to students' ages and developmental stages. The underpinning knowledge and behaviours students learn through the curriculum include the following:

- · How to evaluate what they see online
- · How to recognise techniques used for persuasion
- · Acceptable and unacceptable online behaviour
- · How to identify online risks
- · How and when to seek support
- · How to identify when something is deliberately deceitful or harmful
- · How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks students may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum are taken from the DfE's "Teaching online safety in school" guidance.

The school recognises that, while any student can be vulnerable online, there are some students who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. students with SEND or LAC status. If needed, relevant members of staff, e.g. the SENDCO and Designated Teacher for LAC work together to ensure the curriculum is tailored so these students receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students. When reviewing these resources, the following questions are asked:

- · Where does this organisation get their information from?
- · What is their evidence base?
- · Have they been externally quality assured?
- · What is their background?
- · Are they age appropriate for students?
- · Are they appropriate for students' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Principal and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that students in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any student who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which students feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything students raise during online safety lessons and activities, they will make a report in line with school procedures.

If a student makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in safeguarding school procedures.

APPENDIX TWO - EDUCATING PARENTS

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming
- Exposure to radicalising content
- Sharing of indecent imagery of students, e.g. sexting
- Cyberbullying
- Exposure to age-inappropriate content, e.g. pornography
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Progress evenings
- Newsletters
- Online resources
- Transition Events
- Parent online forums
- Regular Principal Email Bulletins

APPENDIX THREE - PERSONAL SOCIAL NETWORKING

Access to social networking sites is filtered as appropriate in school, and on school devices.

Staff and students are not permitted to use social media for personal use during lesson time.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Staff receive training on how to use social media safely and responsibly.

Staff are not permitted to communicate with students or parents over social networking sites and are reminded to alter their privacy settings to ensure students and parents are not able to contact them on social media.

Where staff have an existing personal relationship with a parent or students, and thus are connected with them on social media, e.g. they are close family friends with a parent at the school, they will disclose this to the DSL or Principal, and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Students are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the safeguarding team and managed in accordance with the relevant policy.

APPENDIX FOUR - RESPONDING TO SPECIFIC ONLINE SAFETY CONCERNS

Cyberbullying

Cyberbullying, against both students and staff, is not tolerated, and incidents are dealt with quickly and effectively whenever they occur. Information about the school's full response to incidents of cyberbullying can be found in the Behaviour Policy.

Online sexual violence and sexual harassment between children (child-on-child abuse)

The school recognises that child-on-child abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

The school responds to all concerns regarding online child-on-child abuse, whether or not the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the Safeguarding team who will investigate the matter in line with the Safeguarding and Child Protection Policy and the Behaviour Policy, where information about the school's full response to these incidents can be found.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose. A "specified purpose" is namely:

· Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear)
· To humiliate, distress or alarm the victim.

Upskirting is not tolerated by the school and incidents of upskirting are reported to the safeguarding team who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy and the Behaviour Policy.

Sexting and the sharing of indecent imagery of students

Sharing indecent imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal. Staff will receive appropriate training regarding child sexual development and will understand the difference between sexual behaviour that is considered normal and developmentally expected, and sexual behaviour that is

inappropriate and/or harmful. All concerns regarding sexting are reported to the safeguarding team.

The safeguarding team will use their professional judgement, in line with the Safeguarding and Child Protection and Policy, to determine whether the incident is experimental, i.e. expected for the developmental stage of the students involved, or aggravated, i.e. involves additional or abusive elements, the images are used recklessly or there is an intent to harm the student depicted. Where the incident is categorised as 'experimental', the students involved are supported to understand the implications of sharing indecent imagery and to move forward from the incident. Where there is reason to believe the incident will cause harm to the student depicted, or where the incident is classified as 'aggravated', the following process is followed:

- The DSL holds an initial fact-finding meeting with appropriate school staff
- Subsequent interviews are held with the students involved, if appropriate
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the student at risk of harm
- At any point in the process if there is a concern a student has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
- The interviews with staff, students and their parents are used to inform the action to be taken and the support to be implemented

When investigating a report, staff members will not view and nude and semi-nude images unless there is a good and clear reason to do so. If a staff member believes there is a good reason to view nude or semi-nude imagery as part of an investigation, they discuss this with the DSL and Principal first. The decision to view imagery is based on the professional judgement of the DSL and always complies with the Safeguarding and Child Protection Policy. If a decision is made to view the imagery, the DSL will be satisfied that viewing:

- is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from any student involved
- is necessary in order to report the image to a website or suitable reporting agency to have the image taken down, or to support the student in taking down the image or in making a report
- is unavoidable because a student has presented it directly to a staff member or nudes or semi-nudes have been found on an education setting's device or network.

Where it is necessary to view the imagery the DSL will:

- Never copy, print, share, store or save images; this is illegal
- Discuss the decision with the Principal
- Undertake the viewing themselves, or make sure viewing is undertaken by another member of the safeguarding team with delegated authority from the Principal
- Make sure viewing takes place with the Principal or another member of the SLT in the room; additional people in the room will not view the imagery
- Only view the imagery on the school premises
- Record how and why the decision was made to view the imagery in line with the Safeguarding and Child Protection Policy

- Make sure that images are viewed by a member of staff of the same sex as the pupil, where appropriate
- Ensure that, if devices need to be passed on to the police, the device is confiscated, disconnected from WiFi and data and turned off immediately to avoid imagery being accessed remotely; the device will be secured until it can be collected by police.

Imagery will not be purposefully viewed where it will cause significant harm or distress to any student involved, in line with the DSL's professional judgement. Any accidental or intentional viewing of imagery that is undertaken as part of an investigation is recorded. Where a staff member has accidentally viewed a nude or semi-nude image, the DSL will ensure they are provided with the appropriate support, as viewing nude or semi nude imagery of students can be distressing.

Online abuse and exploitation

Through the online safety curriculum, students are taught about how to recognise online abuse and where they can go for support if they experience it. The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment. All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the safeguarding team and dealt with in line with the Safeguarding and Child Protection Policy.

Online hate

The school does not tolerate online hate content directed towards or posted by members of the school community. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved.

Online radicalisation and extremism

The school's filtering system protects students and staff from viewing extremist content. Concerns regarding a staff member or student being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty.

Online Hoaxes and Harmful Online Challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the student and the way in which they are depicted in

the video.

The school will ensure that students are taught about how to critically identify when online content is untrue or harmful and how to respond to this content, in line with the Curriculum section of this policy. The SENDCO will assess whether some students, e.g. students who have been identified as being vulnerable or students with SEND, need additional help with identifying harmful online challenges and hoaxes, and will tailor support accordingly.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the school, they will report this to the safeguarding team immediately.

The DSL or DDSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL or DDSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely. The DSL or DDSL will check the factual basis of harmful online challenges or hoaxes against a known, reliable and trustworthy source, e.g. the UK Safer Internet Centre, and will carefully consider if a challenge or story is a hoax or is harmful prior to providing any direct warnings to students or parents.

The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase students' exposure to distressing content, and so will avoid showing students distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.

Where the school's assessment finds an online challenge to be putting students at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant students, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL / DDSL and Principal will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL / DDSL and the Principal will decide whether each proposed response is:

- Factual and avoids needlessly scaring or distressing students
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils that is almost exclusively being shared amongst older students
- Proportional to the actual or perceived risk
- Helpful to the students who are, or are perceived to be, at risk
- Age-appropriate and appropriate for the relevant students' developmental stage
- Supportive.