Online Safety Policy

Chair of Governors: Mrs M Probin

Headteacher: Mrs D Trussell

DOCUMENT CONTROL	
Document Title: **Online Safety Policy**	
Version Number: **3**	Author(s) name and job title: **Mrs H Larkin - Head of Safeguarding & Welfare**
Date Approved: 30th June 2022	Document status: **LIVE**
Effective Date: 1st July 2022	Approved by: Local Governing Body
Superseded Version: **2**	Date of next review: September 2023

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.

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.

Roles and Responsibilities

The **Headteacher** is responsible for:

- Ensuring 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
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping students' safe
- Working with the DSL and governing body to update this policy

The **DSL & Deputy DSL** are responsible for:

- Taking the lead responsibility for online safety in the school
- Acting as the named points of contact within the school on all online safeguarding issues
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that all students face online
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented
- Ensuring safeguarding is considered in the school's approach to remote learning
- Ensuring appropriate referrals are made to external agencies, as required
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff
- Maintaining records of reported online safety concerns and the actions taken in response to concerns
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures
- Reporting to the governing body about online safety

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to
- Modelling good online behaviours
- Maintaining a professional level of conduct in their personal use of technology
- Having an awareness of online safety issues
- Reporting concerns in line with the school's reporting procedure
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum

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.

The curriculum

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

- Health and Wellbeing
- PSHE
- Computing

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

Staff training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction. Online safety training for staff is updated annually and is delivered in line with advice from our local safeguarding partners. In addition to this training, staff also receive regular online safety updates as required and at least annually.

The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the Staff Code of Conduct (The Flixton Way) and the Acceptable Use Agreement at all times, which includes provisions for the acceptable use of technologies and the use of social media. All staff are informed about how to report online safety concerns, in line with safeguarding procedures. The DSL and Deputy DSL act as the first point of contact for staff requiring advice about online safety.

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.

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.

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 signed 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.

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 DSL oversee weekly checks on the filtering and monitoring systems. Reports of inappropriate use, websites or materials are investigated and can be reported to ICT technicians for removal / blocking. Reduced filtering can only be applied with the permission of the Headteacher.

Deliberate breaches of the filtering system are also investigated; If a student has deliberately breached the filtering system, they will be disciplined in line with the Student Discipline Policy, and this will be recorded on CPOMS. If a member of staff has deliberately breached the filtering system, this will be investigated and dealt with by the HR Officer. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

Network Security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. 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.

Emails

Access to and the use of emails is managed in line with GDPR, and the FGS Acceptable Use Agreement. Staff and students are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Any email that contains sensitive or personal information should be sent using secure means – eg initials / abbreviations only when referring to students, and attached documents should be password protected. Computing or PHSE lessons explain email etiquette and safe usage to students.

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.

The School Website

The Headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. Minimum personal information relating to staff and students is published on the website, and always in consultation with the subject. If images are published, we will always have permission to do so.

School-Owned Devices

Staff members may be issued with a computer, laptop, mobile phone or tablet to assist with their work; these devices must be password protected. Students may be provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons, or chromebooks to use at home. Where available, all school-owned devices are fitted with software to ensure they can be remotely accessed in case data on the device needs to be protected, retrieved or erased.

Use of Personal Devices

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

Personal devices are not permitted to be used in the toilets or changing rooms.

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 own 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 Headteacher. 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.

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 Student Services for assistance.

Students' devices can be searched, screened and confiscated in accordance with the Behaviour Policy and the Safeguarding Policy. If a staff member reasonably believes a student's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Managing Reports of Online Safety Incidents

Staff members and students are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

Concerns regarding a staff member's online behaviour are reported to the Headteacher who decides on the best course of action in line with the relevant policies. Concerns regarding a student's online behaviour are reported to the safeguarding team who investigate and then deal with them in accordance with relevant policies depending on their nature, ie. Behaviour Policy and the Safeguarding & Child Protection Policy. 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.

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, 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.

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

The school recognises that peer-on-peer 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 peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer 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.

Remote Learning

All remote learning is delivered in line with the school's Remote Learning Plan.

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, & the Headteacher conduct annual reviews of this policy to evaluate its effectiveness.

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 DSL is involved with the development of the school's online safety curriculum.

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. Relevant members of staff, e.g. the SENCO 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 Headteacher 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:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources
- Transition Events
- Parent online forums

APPENDIX THREE - PERSONAL SOCIAL NETWORKING

Access to social networking sites is filtered as appropriate.

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 Deputy DSL 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.

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 pupils 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 Headteacher 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 Headteacher
- Undertake the viewing themselves, or make sure viewing is undertaken by another member of the safeguarding team with delegated authority from the Headteacher
- Make sure viewing takes place with the Headteacher 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 Wi-Fi 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 SENCO 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 Deputy DSL 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 Deputy DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely. The DSL or Deputy DSL 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 / Deputy DSL and Headteacher 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 / Deputy DSL and the Headteacher 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.