STEEL RIVER
ACADEMY TRUST

Online Safety Policy

Review Date	12.4.21
Review Frequency	1 year
Date for Next Review	1.9.21 (to bring in line with KCSIE)
Author	John Frost

The school has a Designated Online Safety Leader (John Frost), who is responsible for reviewing and updating this policy. They work in collaboration with members of the SLT in order to ensure this policy meets the ever-changing issues relating to the internet and its safe use.

The Online Safety Policy has been written by the school, incorporating points from the Department for Education's (DfE) statutory guidance 'Keeping Children Safe in Education', its non-statutory guidance 'Teaching Online Safety in Schools' and a number of other carefully selected sources. The policy has been agreed by the leadership team and approved by the Governing Body. It will be reviewed regularly. Changes will be made immediately if technological or other developments require it.

Online Safety Risks

The Department for Education published an updated version of 'Keeping children safe in education' in 2020. It states the following:

1. *The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.*

2. *An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.*

3. *The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:*
3.1 *content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;*

3.2 *contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults;*

3.3 *conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.*

4. *Resources that could support schools and colleges include:*
4.1 *Be Internet Legends developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils.*

4.2 *Disrespectnobody is Home Office advice and includes resources on healthy relationships, including sexting and pornography.*

4.3 *Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.*

4.4 *PSHE association provides guidance to schools on developing their PSHE Curriculum.*

4.5 *Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.*

4.6 *Thinkuknow is the National Crime Agency/CEOPs education programme with age specific resources.*

4.7 *UK Safer Internet Centre developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.*

The following sections of this policy address the above risks and the systems in place to reduce the risk both within school and for our children in their home lives.

Filters and monitoring

Statutory guidance from the DfE dictates the following:

5. *Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or college's IT system. Governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Our academy uses the esafe system: https://www.esafeglobal.com/ .Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks. The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.*

5.1 *The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring Guidance on e-security is available from the National Education Network.*

6. *Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises. Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.*

In line with DfE guidance, the school has appropriate filtering and monitoring systems in place. The school's broadband connection is provided by OneIT. The filters in place are extensive and include lists of illegal sites/inappropriate sites that cannot be accessed. It also allows open access and sharing of resources between educational establishments. Use of the web through OneIT's services is monitored and traceable by the network

administrators. In addition to this, there is the consideration that children will inevitably access the internet outside of school. It is therefore vital that we give our children the tools and knowledge to empower them to be safe on the internet and equally as important - to know what to do when they come across any of the dangers. This is addressed further below.

From time to time websites can be blocked even though there are no obvious threats or dangers. Once these have been checked thoroughly by a member of staff, they can contact the OneIT Helpdesk to notify them that a website is suitable for educational purposes. This can be done at: https://helpdesk.oneitss.org.uk/helpdesk/WebObjects/Helpdesk.woa. Staff should ensure that they use their school email account for this purpose.

Searches using the school's network are monitored. The school uses Smoothwall to notify the headteacher of any inappropriate searches or searches which then result in accessing a site with potentially inappropriate content. The headteacher will then follow up any of these breaches and a log is held in the office.

Online Safety Education & Training

Whilst regulation and technical solutions are very important, their use must be balanced by educating users of potential Online Safety risks as well as how to develop safe and responsible behaviours to minimise them, wherever and whenever they go online.

Online Safety education will be provided in the following ways:

Online Safety Training for Staff and Governors

At Whale Hill Primary School we ensure that all teaching and non-teaching staff can recognise and are aware of Online Safety issues. All staff take responsibility for promoting online safety.

Annual training and updates have been delivered previously by Simon Finch, a leader in safeguarding and digital literacy. In February 2017, John Frost completed the CEOP Ambassador training course and has provided staff training since then. In addition to this, staff and governors receive regular training about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding (for example, the Prevent strategy). They are also directed to relevant websites to help support their understanding of these issues. All members of staff are also aware of the documents and policies which have to be updated throughout each year and where their actions need to be monitored and logged (see managing online safety). During each September, each member of staff reviews the policies for both online safety and acceptable use and they also review the statements which underpin their Acceptable Use Agreement and Staff Behaviour Policy.

Online Safety Training for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school provides opportunities for parents/carers to receive online safety education and information (e.g. via the school website, Facebook and Parent Mail) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good online safety behaviour. Each year, 'Parent Welcome' meetings are set up each September to invite parents in to discuss what they should expect over the coming academic year. At these meetings, a member of staff delivers a short online safety presentation on the issues surrounding staying safe online. These meetings include valuable information which includes; cyberbullying, password safety, social networking sites and the use of other gaming media. Parents also receive an up-to-date 'Online Safety Guide for Parents' that has been produced by the school. We also arrange for our parents to receive copies of the 'Digital Parenting' magazine (published by Vodafone and ordered from Parentzone) which covers current and relevant issues linked to the use of internet use when these are published.

Online Safety within the Curriculum

Using searchable cached sites such as Espresso provide a completely safe environment for children to conduct research; however limiting access will not protect children and educate them to be safe on the internet. Therefore it is vital to provide opportunities for children to conduct safe searches.

During any lesson which involves children using the internet, tasks and expectations will be made explicit to children to ensure they aware of what they are and are not allowed to do.

Children will not be allowed to access and search the internet unless authorised by a member of staff. Responsibility for the monitoring of what the children find is then the responsibility of that adult. Details of when the use of searching on the internet is appropriate can be found in the school scheme of work for computing; other uses are the sole responsibility of the supervising adult.

Accessing and interacting with the internet is a key aspect of many users' reasons for having an internet connection. Simply preventing the children from using internet is not preparing them for the real world (including for use at home). Therefore, online safety is implicitly taught throughout school and referred to whenever a unit of work requires use of the internet.

Online Safety objectives are embedded throughout the computing curriculum (which includes dedicated lesson time for online safety) and the PSHE curriculum. In Key Stage 2, 'Digital Leaders' are also trained in the key aspects of online safety with the aim of them helping to support other pupils and also parents at scheduled events.

Cyberbullying

Cyberbullying is referenced in the Multi-Academy Trust's Anti-Bullying Policy though a more detailed explanation is offered here. Cyberbullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.

By cyberbullying, we mean bullying by electronic media:

- Bullying by texts, messages or calls on mobile phones.
- The use of mobile phone cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites.
- Using e-mail to message others inappropriately.
- Hijacking/cloning e-mail accounts.
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms and social networking sites.
- Impersonating others on social networking sites by creating fake profiles or hijacking accounts.

Whale Hill Primary School embraces the advantages of modern technology in terms of the educational benefits it brings. However, the school is mindful of the potential for bullying to occur. Central to the School's anti-bullying policy is the belief that 'all pupils have a right not to be bullied' and that 'bullying is always unacceptable'. The school also recognises that it must take note of bullying perpetrated outside school which spills over into the school.

Cyber-bullying is generally criminal in character. The law applies to cyberspace as outlined below:

- It is unlawful to disseminate defamatory information in any media including internet sites.
- Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
- The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

Whale Hill Primary School educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through the PSHE and computing curriculums and assemblies, continue to inform and educate its pupils in these fast changing areas.

Whale Hill Primary School trains its staff to respond effectively to reports of cyberbullying or harassment and has systems in place to respond to it. We endeavour to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems. No pupil is allowed to work on the internet in the computer suites, or

any other location within the school - which may from time to time be used for such work - without a member of staff present.

Whilst education and guidance remain at the heart of what we do, Whale Hill Primary School reserves the right to take action against those who take part in cyberbullying. All bullying is damaging but cyberbullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts. Whale Hill Primary School supports victims and, when necessary, will work with the police to detect those involved in criminal acts. Whale Hill Primary School will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, either inside or outside of school.

Whale Hill Primary School will use its power of confiscation, to include internet and learning platform access, where necessary to prevent pupils from committing crimes or misusing equipment.

All members of the School community are aware they have a duty to bring to the attention of the Head teacher any example of cyber-bullying or harassment that they know about or suspect.

Dealing with exposure to inappropriate materials: content, contact and conduct

Guidance to staff

If you suspect or are told about a content, contact or conduct, including cyber-bullying, incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone.
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names.
- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image (if appropriate).
- Go with the pupil and see the Head teacher, or in her absence, a member of the Senior Leadership Team.

Computers

- Ask the pupil to get up on-screen the material in question (if this is not possible the child could tell you how to find it on the screen and the website they were working within).
- Ask the pupil to save the material (if appropriate).
- Print off the offending material as a record (cyberbullying).
- Make sure you have got all pages in the right order and that there are no omissions.

- Accompany the pupil, taking the offending material, to see the Head teacher.
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

Guidance for Pupils

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, a teacher or your headteacher.
- Do not answer abusive messages but log and report them.
- Do not delete anything until it has been shown to your teacher, parents/guardian or the headteacher (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying).
- Do not share personal IT details.
- Never reply to abusive e-mails, messages or texts.
- Never reply to someone you do not know.

Guidance for Parents

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyberbullying:

- Parents can help by making sure their child understands the school's policy and, above all, how seriously Whale Hill Primary School takes incidents of cyber-bullying.
- Parents should also explain to their sons or daughters legal issues relating to cyberbullying.
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents should contact the Head teacher as soon as possible. A meeting can then be arranged, which may involve other relevant members of staff.

If any teacher, pupil or parent suspects that any of our children are at heightened risk of exposure to inappropriate use of the internet, they should inform the Designated Safeguarding Leads as a priority.

Safeguarding Against Radicalisation and Extremism

At Whale Hill Primary School, we consider protecting children against radicalisation and extremism is part of the school's wider safeguarding duties and is similar in nature to protecting children from grooming. This can include other risks such as drugs, gangs, neglect and sexual exploitation. We also acknowledge that some children may be vulnerable to radicalisation and, to fulfil our Prevent duty, we ensure that staff are able to identify such children. We have a vital role to play in protecting our pupils from the risk of extremism and radicalisation.

Keeping children safe from the risks posed by terrorist exploitation of social media should be approached in the same way as safeguarding children from any other form of online abuse.

At Whale Hill, if there are concerns over a child's safety at risk of radicalisation, Whale Hill Primary School, will adhere to the following:

- In the first instance, our schools safeguarding policy will be adhered to.
- The local police lead for anti-terrorism will be informed.
- If the threat is imminent, and there is a concern that a child's life is in immediate danger, or that they may be planning to travel to Syria or Iraq, the risk is heightened and therefore an emergency call must be made – 999 or 0800789321 (Anti-Terrorist Hotline)
- Following a concern with regards to radicalisation and extremism the local authority or police might suggest a referral to the 'Channel' programme, which is a voluntary government funded programme which aims to safeguard children and adults from being drawn into terrorist activity.

More detail is provided in the school's Safeguarding Against Radicalisation and Extremism policy.

Online Safety at home

In line with the school's approach to all aspects of safeguarding, parental engagement is considered essential in ensuring children are safe online. The school believes that parents are their children's first and best teachers and that they need to be equipped with the knowledge and skills to support their children at home. As discussed above, weekly updates on an aspect of online safety relevant to primary school children are sent home via Parent Mail. In addition, more detailed half-termly resources are provided, for example our 'Online Safety Leaflet for Parents' and Vodafone's 'Digital Parenting' magazine.

Several sites offer helpful advice to parents, particularly with respect to how they can best monitor their child's use of the computer at home. Some examples of important and useful information that the school has shared with parents can be found on the following sites:

- www.thinkuknow.co.uk/
- www.saferinternet.org.uk
- www.net-aware.org.uk
- www.parentzone.org.uk
- http://vodafonedigitalparenting.co.uk/

Managing Online Safety in School

There are a number of documents adhered to within school which audit the effectiveness of Online Safety within Whale Hill Primary School:

Online Safety Policy – audited annually by all members of staff.

Acceptable Use Policy – audited annually by all members of staff.

Staff Behaviour Policy – updated with any new members throughout the year.

Home-School Agreement– signed by parents, children and teachers to ensure the standards and expectations of the school are upheld by all parties.

Accidental Access to Inappropriate Materials – updated as and when necessary.

Website Unblocking – updated as and when necessary once the OneIT helpdesk has been notified.

Use of Personal Digital Devices within School – A document to log staff using their own devices either within school or on trips. Devices to be checked by John Frost or a member of SLT afterwards to ensure any images of the children have been removed.

Online Safety and Unacceptable Use Incident Log – All Online Safety and unacceptable uses of the internet including social networking sites are to be logged in here. This log is then monitored by the head teacher termly.

Form of Consent for Use by the School and media of Photographs of Children – A document that must be signed by parents and carers for permission to use photographs and videos of children on the school website or social media. Without consent, images may not be used for these purposes. Consent is obtained annually.

Further information regarding Acceptable Use Policies and Digital Images can be found within the School's Acceptable Use Policy outlined in the Computing Policy.

<u>Use of technology for online / virtual teaching</u>

The Safer Recruitment Consortium (2020) issued an update relating to the increase in virtual teaching due to school closures during the Covid-19 outbreak. In the case of such an event, and any future event which may require the use of virtual teaching, guidance for staff is outlined below:

All settings should review their online safety and acceptable use policies and amend these if necessary, ensuring that all staff involved in virtual teaching or the use of technology to contact pupils are briefed on best practice and any temporary changes to policy / procedures. When selecting a platform for online / virtual teaching, settings should satisfy themselves that the provider has an appropriate level of security.

Wherever possible, staff should use school devices and contact pupils only via the pupil school email address / log in. This ensures that the setting's filtering and monitoring software is enabled. In deciding whether to provide virtual or online learning for pupils, senior leaders should take into account issues such as accessibility within the family home, the mental health and wellbeing of children, including screen time, the potential for inappropriate behaviour by staff or pupils, staff access to the technology required, etc.

Virtual lessons should be timetabled and senior staff, DSL and / or heads of department should be able to drop in to any virtual lesson at any time – the online version of entering a classroom. Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents.

The following points should be considered:-

- *think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred*
- *staff and pupils should be in living / communal areas – no bedrooms*
- *staff and pupils should be fully dressed*
- *filters at a child's home may be set at a threshold which is different to the school*
- *resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content.*

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary. Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and pupil AUPs should clearly state the standards of conduct required.

If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.

For home learning, Whale Hill used Parent Mail during the first Covid-19 Lockdown before moving to Seesaw due to its interactive design and features. These offer secure and reliable contact with parents. When sending home learning resources and contacting parents, staff devices have been used either in school or securely connected to the school network from home. Tasks sent directly to parents and children through Seesaw with instructions were initially favoured over virtual lessons so that parents are able to support children academically as well as help them to use online resources safely and responsibly. After reviewing the effectiveness of home learning during the second Covid-19 Lockdown, some activities were supplemented with live teaching and whole-year group assembly sessions. These were received positively by children and parents. More details are included in the schools Remote Learning Policy.

When telephone contact has been made with parents, it has been strongly encouraged that this be done in school and using the school's telephone. Staff who have chosen to telephone parents from home, it has been made clear that personal details be withheld using the phone's settings or by dialling with the prefix '141'.

Acknowledgements:

Keeping children safe in education: Statutory guidance for schools and colleges. (2020) Department for Education. *https://www.gov.uk/government/publications/keeping-children-safe-in-education--2* [Accessed 2 April 2021]

Teaching online safety in schools: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects. (2019) Department for Education. *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf* [Accessed 7 April 2021]

Revised Prevent duty guidance: for England and Wales (2021) Home Office. *https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales* [Accessed 7 April 2021]

Guidance for safer working practice for those working with children and young people in education settings. (2020) The Safer Recruitment Consortium. *https://www.saferrecruitmentconsortium.org/GSWP%20COVID%20addendum%20April%202020%20final-2.pdf* [Accessed 4 April 2021]

Guidance for safer working practice for those working with children and young people in education settings: COVID addendum April 2020 (2020) Safer Recruitment Consortium. *https://www.saferrecruitmentconsortium.org/GSWP%20COVID%20addendum%20April%202020%20final-2.pdf* [Accessed 7 April 2021]