



Streetsbrook Infant & Early Years Academy



Online Safety Policy

Streetsbrook Infant and Early Years Academ

'Learning for Life'

At Streetsbrook, we strive to provide an equal chance for all to become responsible citizens who lead happy and fulfilled lives, and are equipped with the skills and abilities to shape the world they live in.

Our values are:

Desire to Learn

To enjoy the lifelong process and challenge of learning; alone and with others

Love and Respect

To have respect for ourselves, others and the environment, recognising and celebrating individual lifestyles, cultures and faiths

Happiness

Developing successful relationships where individuals can build and follow their dreams

Confidence

Having the self-belief to embrace and follow your own choices.

Being a Good Citizen

Making a positive contribution to communities on a local and global scale

Contents

Statement of Intent	1
Defining 'Online Safety'	1
Legal Framework.....	1
Roles and Responsibilities	2
Managing Online Safety	3
Cyberbullying.....	5
Child-on-Child Sexual Abuse and Harassment	5
Grooming and Exploitation	6
Mental Health	7
Online Hoaxes and Harmful Online Challenges	7
Cyber-Crime	8
Online Safety Training for Staff	8
Engagement and Education of Staff	9
Online Safety and the Curriculum	9
Use of Technology in the Classroom	10
Use of Smart Technology	10
Educating Parents	11
Internet Access	12
Using the Internet to Enhance Learning.....	14
Using Information from the Internet	14
Community Use of ICT and the Internet.....	16
Filtering and Monitoring Online Activity	16
Network Security	17
Maintaining the Security of the School ICT Network and Services	17
Emails	18
Social Networking.....	19
The School Website.....	19
Use of Devices	19
Remote Learning	21
Monitoring and Reviewing	23

Appendix 1 Online Safety Risk Assessment

NB – the Model Online Safety Policy produced by The School Bus has been used to support the writing of this policy.

Statement of Intent

Streetsbrook Infant & Early Years Academy understands that using online services is an important aspect of raising educational standards, promoting pupil 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 pupils and staff.

The breadth of issues classified within online safety is 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, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils 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 pupils and staff.

Defining 'Online Safety'

Online Safety is about educating children and young people to use technologies in ways which will keep them safe but without limiting their opportunities for creation and innovation, whilst working or playing on the Internet.

Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Managing Allegations Against Staff Policy
- Acceptable Use Agreement
- Cyber-Security Policy
- Disaster Recovery Policy
- EASEE
- Child Protection and Safeguarding Policy, including PREVENT
- Behaviour Policy, including Anti Bullying
- Disciplinary Policy and Procedures
- Data Protection Policy
- Staff Guidelines, including Code of Conduct and Confidentiality
- Photography and Images Policy
- Mobile Devices Policy
- Remote Education Policy

Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

The Headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- 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.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- 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.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Maintaining records of reported online safety concerns as well as 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 board about online safety on a termly basis. The head teacher shall report to the governors.
- Working with the head teacher and governing board to update this policy on an annual basis.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members will be 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.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- 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.

Children will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school 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.

Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Annual Safer Internet Day
- Annual Safer Internet Day assembly
- 'Izzy Ipad' Online Safety starters
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Daily informal conversations with children about safety
- Weekly Newsletters

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

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. If the concern is about the Headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and ICT technicians, and manages concerns in

accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising children, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against children or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Child-on-child sexual abuse and harassment

Children may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that children are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware

that allowing such behaviour could lead to a school culture that normalises abuse and leads to children becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that children who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the child may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact children are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a child may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain children at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a child's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a child is suffering from challenges in their mental health. Concerns about the mental health of a child will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

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 pupil and the way in which they are depicted in the video.

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

The 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 pupils, 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 will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

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

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing children.

- Not inadvertently encouraging children to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger children but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the children who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The 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 pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that children with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a child's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that children are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Engagement and education of Staff

The school's Online Safety Policy will only be effective if all staff subscribe to its values and methods. Therefore, teaching students and cover or supply staff should not be asked to take charge of an Internet activity without full and proper preparation with a member of the school's teaching staff.

All staff will be given the school Online Safety Policy and its importance explained. Staff development on Online Safety will be provided when required. A copy of the policy can additionally be found in the school's network, under the policies folder on the 'teachers' drive'. The Online Safety Policy will also be published on the school's website.

All staff must abide by the rules stated in the Acceptable Use Policy. (See appendix ii) Staff should be aware that Internet traffic is monitored and traced to the individual user. Discretion and professional conduct is therefore essential when using the Internet for both professional and personal use both on and off school premises.

Staff must not knowingly access or download pornographic, offensive, defamatory or other illegal material available on the Internet. This will be treated as a serious disciplinary offence and may lead to dismissal.

Online safety and the curriculum

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

- PSHE
- Computing
- Any lesson where iPads are used by children. This may include conducting research during subjects such as History and Geography

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Every computing lesson at Streetsbrook Infant & Early Years Academy begins with an explicit online safety starter scenario.

Pupils 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. The underpinning knowledge and behaviours pupils 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
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in [appendix A](#) of this policy.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that children who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will 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 will consider the topic that is being covered and the potential that children in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any child who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil 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 will ensure a safe environment is maintained in which children 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 children raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil 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 the Child Protection and Safeguarding Policy.

Use of technology in the classroom

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

- iPads
- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras
- Interactive smart boards

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that children use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Children will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Children will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the school's Staff ICT and Electronic Devices Policy.

The school recognises that Children's unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for children.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Children will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban a child's use of personal technology whilst on school site. At Streetsbrook Infant & Early Years Academy we consider the young age of our children, we do not expect them to bring their own devices into school.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Educating Parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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 pupils, 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 will be raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources
- Information evenings
- Website resources

Streetsbrook Infant and Early Years Academy recognise that Parents/carers have an essential role to play in enabling children to become safe and responsible users of the Internet and digital technology.

Data will be being collected from the Health Related Behaviour Questionnaire, (HRBQ), conducted at Streetsbrook of Year 2 children bi-annually. This is due to take place in March 2023 and will include questions regarding internet use.

Parents'/carers' will have access to the school Online Safety Policy and updates will be regularly shared in newsletters, letters, the school brochure, school website and within curriculum meetings.

A partnership approach to Online Safety both at home and at school will be encouraged through:

- consultation with the Parent Partnership Team;
- a letter will be sent out to Parents at the beginning of each academic year to raise awareness of the importance of Online Safety;
- other information and guidance for Parents on Online Safety will be made available throughout the academic year;
- providing Parents with access to Online Safety workshops or meetings
- Parents/carers will be encouraged to role model positive behaviour for their children online;
- Parents seeking additional information to safeguard their children when using the Internet will be referred to organisations listed on the school's website.

Any Internet issues that arise in school will be handled sensitively to inform parents without alarm.

Internet access

Children, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

All members of the school community will be 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.

Ensuring Internet access is appropriate and safe

The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- all Internet devices are filtered and monitored by the local authority whom regularly monitor, filter and review blocked content;

- children will be taught that they might not have similar filtering systems at home and that they need to self-regulate their own uses of the Internet;
- children using the Internet will normally be working in the classroom, during lesson time and will be supervised by an adult, (usually the class teacher), always;
- staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of the pupils;
- staff will be vigilant when children are undertaking their own search and will check that the children are following the agreed search plan;
- children will be taught to use email and the Internet responsibly to reduce the risk to themselves and others;
- children will have signed an Acceptable Use Agreement;
- the Computing coordinator and IT Technician will monitor the effectiveness of Internet access strategies;
- the Headteacher will ensure that the Online Safety Policy is adhered to by all members of staff;
- an Online Safety training programme will be delivered to all children to raise the awareness and importance of safe and responsible use of the Internet and other electronic communication tools.
- When working online children will be taught to be S.M.A.R.T:
Safe- to remain safe by protecting personal information
Meeting- never meet somebody you have only been in touch with online without a parent or guarding
Accepting- do not accept email, files or messages from people you do not know
Reliable- not all information on the Internet is true, including the identify of others
Tell- it is never too late to tell a parent, carer or responsible adult if someone or something makes you feel afraid online.
- Each year, Streetsbrook celebrates Safer Internet Day and the children participate in activities that promote safe and acceptable Internet use. Each year there is a different focus to promote the slogan 'together for a better internet'.

Despite high levels of filtering, children and staff may occasionally be confronted with inappropriate materials. If staff or children discover unsuitable sites, the URL (address), time, date and content must be reported to Solihull ICT Services, and the academy's Online Safety Lead, (Miss Neeve Cartwright).

Internet access in school

Providing access to the Internet in school raises educational standards and supports the professional work of staff.

Parents/carers will be informed that children will be provided with supervised Internet access. However, to meet the needs of our most able children and to encourage independent learning some children, following appropriate teaching and agreement of a search plan, will have access to the Internet for independent research.

The school will maintain a current record of all staff and children who are granted Internet access, all of whom must read, sign and abide by the 'Acceptable Use Policy,' see appendix (ii), before using

any school ICT resource. The use of computer systems without permission or for inappropriate purposes could constitute in a criminal offence under the Computer Misuse Act 1990.

Similarly, to other media such as magazines, books and videos, some material available on the Internet is unsuitable for pupils. Streetsbrook Infant and Early Years Academy will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material, whilst using the Internet.

However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither Streetsbrook Infant and Early Years Academy nor SMBC can accept liability for the material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly.

Using the Internet to enhance learning

Access to the Internet will become a planned part of the curriculum that will enrich and extend learning activities and will be integrated into the class schemes of work. Access levels are reviewed to reflect the curriculum requirements and age of the children. The school's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of children provided by the LA.

As part of the school's computing scheme of work for KS1, children will be taught what Internet use is acceptable and what is not. We recognise that pupils learn most effectively when they are given clear objectives for Internet use. All children will learn how to use a web browser and are taught to use Kiddle or KidRex, which are safe search engines. Children will be educated in how to use the named Internet search engines to find and evaluate information. **There will always be an adult present when the children are accessing the Internet.**

Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the children:

- access to the Internet may be by teacher/teaching assistant demonstration;
- children may access teacher-prepared materials, rather than the open Internet;
- children may be given a suitable web page or a single website to access;
- children may be provided with lists of relevant and suitable websites which they may access;
- children may be allowed to undertake their own Internet search having agreed a search plan with their teacher.

Using information from the Internet

Streetsbrook believes that in order to use information from the Internet effectively, it is important for children to develop an understanding of the nature of the Internet and information available on it.

Children need to understand how to extract, interpret and use information and evaluate its significance. Respect for copyright and intellectual property rights will also be taught. The academy will ensure that the copying and subsequent use of Internet derived materials by staff and children comply with the copyright law.

Children

Children will be educated about the importance of keeping personal information private from the beginning of school. Children are taught never to give out personal details of any kind which may identify them or their location, for example their full name, address, mobile or landline numbers, school, IM address, email address, names of friends, specific interests and clubs etc., when using the Internet.

Children should be advised on security and encouraged to set passwords and deny access to unknown individuals and unwanted communications. Children are advised not to place personal photos on any social network space and to not publish specific detailed private thoughts.

Streetsbrook is aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to view the bully's comments. Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.

Staff

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Teachers' official blogs or wikis should be password protected and only run from the school website or the SMBC extranet. Teachers should not run social network spaces for students on a personal basis or communicate with children through private social networking sites, even on educational matters, but should use official sites sanctioned by the school.

When using social networking sites for personal use, teachers must maintain school confidentiality and not publish school specific information. Staff must not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role.

Internet and Education

The Internet is an essential element in the 21st century life for education, business and social interaction and its use is part of the statutory curriculum, a necessary tool for learning.

The purpose of Internet use in school is to:

- raise educational standards;
- promote pupil achievement;
- support the professional work of staff;
- enhance the school's management functions.
- develop essential skills to ensure children are 'Life Ready.'

Therefore, Streetsbrook has a duty to provide teachers and children with quality Internet access as part of their teaching and learning experiences.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums, art galleries and to experts in many fields for children and staff;
- inclusion in the National Education Network, connecting all UK schools;
- educational and cultural exchanges between children world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with SMBC and DfE;
- access to learning wherever and whenever convenient.

Children and young people may expose themselves to danger, whether knowingly or unknowingly, when using the Internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate or possibly illegal. We have a responsibility to educate our children and teach them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies. We work with our parents to raise awareness of online safety, including them as much as possible in this process so that they can ensure that any access the pupils have to computers and Internet at home is safe.

Community Use of ICT and the Internet

Where appropriate the school will liaise with local organisations to establish a common approach to Online Safety. The school will be sensitive to Internet related issues experienced by children out of school, e.g. social networking sites, and offer appropriate advice. The Internet is available in many situations within the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café. Ideally, young people would encounter a consistent policy to Internet use wherever they are.

In community Internet access, there is a fine balance to be achieved in ensuring 'freedom of information,' whilst providing adequate protection for children and others who may be offended by inappropriate material. Each organisation is developing access appropriate to its own client groups and children may find variations in these rules and even unrestricted Internet access. Although policies and practices may differ, community partners adhere to the same laws as schools with respect to content copyright and misuse. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with children on the reasons for the differences would be worthwhile. Children need to know how to stay safe online wherever they are.

Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools'

and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

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.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and children will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Staff members will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users will be required to lock access to devices and systems when they are not in use.

Full details of the school's network security measures can be found in the Cyber-security Policy.

Maintaining the security of the school ICT network and services

We recognise that the connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

Streetsbrook Infant and Early Years Academy currently works in partnership with Solihull MBC to ensure that filtering systems are as effective as possible. The IT Technician will evaluate filtering systems regularly and ensure that necessary updates are installed so that the systems are as effective as possible. Solihull MBC uses a blocking strategy to prevent access to a list of unsuitable sites.

Maintenance of the blocking list is a major task, as new sites appear daily and therefore, if staff or children discover unsuitable sites, the URL, time and date must be reported to the school Online Safety Leader without delay. In addition to informing the Online Safety Leader, any material that the school believes is illegal must be reported to appropriate agencies such as IWF and CEOP immediately.

The security of the school information systems will be reviewed regularly and antivirus protection will be updated regularly. All security strategies will follow Solihull MBC guidelines.

The IT Technician regularly reviews system capacity and files held on the school's network are regularly checked. Unapproved system utilities and executable files will not be allowed in children's work areas or attached to emails.

Portable media may not be used without specific permission followed by a virus check. The school will supply each member of staff with a password protected flash drive. However, children's personal information should not be stored on any portable media.

Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff and children will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and children must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

Using email

Email use can bring significant educational benefits and interesting projects between neighbouring schools or even continents. As part of the curriculum, children will be taught basic email conventions. However, unregulated email can provide routes to children that bypass the traditional school boundaries and spam, phishing and virus attachment make email an important Online Safety issue.

As with social networking, email can be used to bully others. Incidents of bullying through email will be dealt with in line with the school policies on behaviour and anti-bullying.

The following rules and guidelines for the use of the school's email system should always be followed:

- children may only use approved email accounts on the school system;
- children must immediately tell a teacher if they receive an offensive email;
- children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission;

- use of words included in the filtering/checking 'banned' list will be detected and logged by SMBC EICT Services;
- excessive social email use can interfere with learning and may be restricted;
- email sent to external organisations by children should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- the forwarding of chain letters is not permitted;
- email addresses should be published carefully, to avoid spam harvesting;
- staff and governors must use their school email for school-related work.

Social networking

The use of social media by staff and pupils will be managed in line with the school's Social Media Policy and staff guidelines. Expectations regarding safe and responsible use of social media will apply to all members of Streetsbrooks' community and exist to safeguard both the school and wider community, on and offline.

Social networking sites and newsgroups will be blocked unless a specific use is approved.

The school website

The Headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The academy website must comply with the academy's guidelines for publications including respect for intellectual property rights and copyright. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. All materials for publication on our website must be, prior to publication, reviewed and authorised by the Headteacher.

The contact details on the website should only include the academy address, email and telephone number. Staff and children's personal information will not be published, to avoid spam harvesting and to uphold individual safeguarding.

Photographs that include children and/or staff add a liveliness and interest to a website. Nevertheless, the security of all children and staff is paramount.

Children's full names will not be used anywhere on the website, particularly in association with photographs. Permission from parents on their consent to publish photographs of their child/ren on the website, must be obtained when joining the school. Teaching staff will check that children in photographs proposed to be placed on the academy website, have parental consent, **before** publication.

Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff guidelines.

Mobile Phones and children

Unfortunately, there are currently now instances of mobile phone camera images being used inappropriately to bully children in other schools. At Streetsbrook, we hope to prevent such issues affecting our school. Consequently, the expectation is that children do not have access to mobile phones. This includes access to mobile phones on school trips.

Mobile Phones and adults

Staff are allowed to bring mobile phones on site, but they must be turned off or be on silent mode throughout the school day. Mobiles should be placed in a container outside the Head's office and remain there for the duration of the day. Streetsbrook Childcare staff should similarly leave their mobiles in the Childcare Manager's office for the duration of the day. During the hours where children are on site, phones are only allowed to be used in the staffroom, where children cannot enter.

On a normal school trip, it is expected that staff will carry a mobile phone. In these circumstances to protect staff members, it is important to consider where and how phones are used. It may be advisable to use the phone near to another member of staff/adult if children are present, or to make the phone call away from the children. Mobile phones and other personal cameras are not to be used for taking photos of children, **unless authorisation has been given by the Headteacher.**

All visitors to Streetsbrook are made aware of the procedures around use of mobile phones, cameras, tablets etc. and should likewise act in accordance with this policy.

School laptops

Teaching staff have been issued a school laptop to use at home to complete tasks, which may include use of the Internet. All issued laptops, have been encrypted to prevent access to unauthorised individuals in the event of a theft or loss of the laptop. It is part of the Acceptable Use Policy for staff, that the Internet and laptops are used responsibly and professionally.

When employment ceases with Streetsbrook, it is expected that an issued laptop is returned promptly to school.

Video Cameras/Video Conferencing and VoIP (Internet Telephony)

To protect staff from any sort of allegation, staff should not use their own cameras or video cameras to record the children in school.

Images taken on the school iPads, once used or printed, should be removed from laptop, iPads, cameras and cloud storage apps such as OneDrive.

Whenever taking photographs, staff must always check the register of children who have been refused permission by their parents to have photographs taken of them. Staff should be then aware of how they use such images.

Video conferencing is a challenging activity with a wide range of learning benefits. Video conferencing sites such as Skype For Business are often used whole-class, to communicate with wider professionals in different fields of work, to enhance understanding of a topic.

Children should ask permission from the supervising teacher before making or answering a video conferencing call. All video conferencing must be supervised by the class teacher and must be authorised by parents and guardians before their children take part in video conferences.

Preparation and evaluation are essential to the whole activity. It is essential to establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class. If the school acquires video conferencing or VoIP hardware the following guidelines should be considered.

All video conferencing equipment in the school must be switched off when not in use and not set to auto answer. IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Use over the non-educational network cannot be monitored and controlled. Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.

External IP addresses should not be made available to other sites and video conferencing contact information should not be put on the school website.

School video conferencing equipment should not be taken off school premises without permission. The equipment must be secure and if necessary locked away when not in use. Responsibility for the use of the video conferencing equipment outside school time needs to be established with care. Only key administrators should be given access to the video conferencing passwords details for the educational video conferring services should be issued to members of staff and kept secure.

When recording a lesson, written permission must be obtained from all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material must be stored securely and if third-party materials are to be included, these must be checked to avoid infringing the owners' Intellectual Property Rights. (IPR)

During Christmas and special events, the school currently allows parents to photograph and video children. Parents are reminded that all photographs and videos should remain their own private property and should not be uploaded to any social networking sites.

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. These emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

iPads are licensed to be used by Early Years and Childcare staff as part of assessment. In addition to staff iPads, the school has at least thirty iPads which can be timetabled to be used as part of lessons throughout the week by the children. All iPad use will be monitored and rules for their use clearly reinforced with the children.

Remote Learning

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

Procedures to follow in case of an incident

If there is an incident in which a child is exposed to offensive or upsetting material the school will respond quickly but calmly to the situation. Responsibility for handling incidents involving children will be taken by the class teacher, who will complete the reporting log form and communicate **immediately** with the Headteacher, (see appendix iii). Staff should treat any online safety concerns in line with the schools Safeguarding procedures and policy. This will involve completing a CPOMS report.

- If a child discovers (view) inappropriate material the first priority will be to give them appropriate support.
- A member of the SLT, preferably the Headteacher and Online Safety Leader, (Miss Neeve Cartwright), must be informed immediately.

- If staff or children discover unsuitable sites, the IT Technician will be informed and he will report the URL (address) to SMBC, who will block the webpage.
- If it is thought that the material is illegal, after consultation with SMBC, the site will be referred to the police.
- If children abuse the privileges of access to the Internet or use of email facilities by failing to follow rules they have been taught or failing to follow the agreed search plan when given the privilege to undertake their own internet search, then sanctions will be taken.
- This may involve a warning at first, before then informing the parents. Teachers may also consider whether access to the Internet may be denied for a period of time.

Protecting personal data

Personal data will be recorded, processed, transferred and made available in compliance with the Data Protection Act 1998. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data, (information that will identify an individual).

The eight principles are that personal data must be:

- processed fairly and lawfully;
- processed for specified purposes;
- adequate, relevant and not excessive;
- accurate and up-to-date;
- held no longer than is necessary;
- processed in line with individual rights;
- kept secure;
- transferred only to other countries with suitable security measures.

Online Safety Complaints

Parents and children will need to work in partnership with staff to resolve issues of Online Safety as they arise. Online Safety complaints will be dealt with using the normal complaints processes for Streetsbrook. Potential child protection or illegal issues, however, must be referred to the school Designated Member of Staff for Child Protection, Mrs Louise Minter. A senior member of staff will deal with formal complaints of Internet misuse. Any complaint about staff misuse of the Internet must be referred to the Headteacher who will use the agreed SMBC procedures.

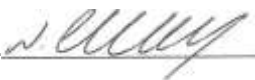
Monitoring and reviewing

The governing board, headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy will be in the Autumn Term 2024.

N Cartwright
Leader for Computing
November 2023

This policy was ratified by the Governing Body on 7 December 2023

Signed  Chair of Governors

Signed  Headteacher

Appendix (i)

SOLIHULL MBC HEALTH & SAFETY RISK ASSESSMENT

ACTIVITY / AREA COVERED BY THIS ASSESSMENT: **Online Safety**

DIRECTORATE / DIVISION / SECTION: **Streetsbrook Infant and Early Years Academy
(Whole-school)**

Impact/severity	High	6	7	9
	Med	3	5	8
	Low	1	2	4
		Low	Med	High
Likelihood				

Hazard	Persons at Risk	Risk Description	Gross / Initial risk		Risk Level	Current Mitigating Action (Existing Controls /Precautions)	Net risk		Risk Level	Owner
			Likelihood	Impact / Severity			Likelihood	Impact/Severity		
A child reveals their private password	All	A child reveals their password to a friend as they log onto the computer or onto their email account.	High	Low	4	Class teacher to remind the children about the importance of keeping passwords private and that if they are struggling to input their passwords then they should ask a teacher for support.	High	Low	4	
An image, text or video has been viewed that makes the child feel scared, anxious or uncomfortable, including adverts	All	When on the Internet, a child might view an image, text or video that makes them feel uncomfortable. This can include clicking or viewing an advert that is on a certified website.	Low	High	6	The school Internet access is designed for educational use and has high level, appropriate filtering and monitoring. Internet usage is mostly guided by the class teacher. Where independent searches on the Internet have been agreed, search plans are discussed with the children and child-friendly search engines agreed to be used. Class teachers will additionally monitor the websites that the children are using.	Low	High	6	

A child has received an email off an unknown sender	All	Whilst accessing email, a child has received an email off an unknown sender.	Low	High	6	Children's school emails should only receive emails from members of staff or fellow children. The child's email address should only be accessed and made available to those within the school setting.	Low	High	6	
Personal information (phone numbers, addresses) have been shared to unknown receivers	All	A child might share personal information to another Internet user.	Low	High	6	Available websites at school do not provide opportunities for children to share information with strangers. The children's email systems should only receive emails that are from staff or other children. Children are to be taught of the importance to keeping personal information private and potential consequences of sharing this.	Low	High	6	
A child has received a nasty message or email	All	A child opens an email that contains a nasty or abusive email.	Low	High	6	Children's email systems are set up so that they should only receive emails from staff or other children. Should the nasty message be sent from a child in the same school, the teacher is to deal with the sender of the message in line with the school behaviour policy and logged in class concern book. This should then be followed up via Child Protection DMS if necessary.	Low	High	6	
Receiving a video message received from an unknown source	All	Whilst connected via video messaging, a request for a video message is received from an unknown source.	Low	High	6	Video messaging is to be run through Solgrid connect, which ensures peer to peer safety.	Low	High	6	
A child has downloaded a virus or spyware system	All	Whilst opening an email or viewing a webpage, a virus or spyware system has been unintentionally downloaded.	Low	High	6	Solgrid checks for viruses in the attachments of incoming and outgoing external email. Websites that provide risk of viruses or spyware are filtered by Sophos.	Low	High	6	

A child might inform an adult about something they have accessed at home that is not age appropriate	All	A child discloses to an adult, (or an adult overheard a child telling their friend), that they have viewed something at home that is not appropriate for their age.	Medium	Medium	5	Depending on the severity, the class teacher should log the concern on an incident report which should then be followed up via the Child Protection DMS if appropriate.	Medium	Medium	5
ASSESSED BY (PRINT) <u>Miss Neeve Cartwright</u>		SIGNED <u>N. Cartwright</u>		DATE ASSESSED 30/11/23					
MANAGER (PRINT) <u>Mrs Louise Minter</u>		SIGNED <u>L. Minter</u>		DATE 30/11/23					