Rose Hill Primary School

Online Safety Policy

February 2020

Date Ratified	Signed By/Position	Signature
Feb 2020	**Head Teacher:** Sue Vermes	
	Chair of Governors: Ailsa Granne	
	Lead Member of Staff: Peter Mallam	
	Lead Member of Staff: Jane Birchenough	
Review Date: Feb 2021 **Please see ANNEX 1 - taken from Covid-19 updated Safeguarding Policy that has been produced by the Education Safeguarding Advisory Team.**		

Vision

We are living in an increasingly connected world where, alongside the benefits of access to technology, come increased risks to children. Lack of guidance and learning in online safety can mean children are unaware of the unintended consequences of their on-line behaviour or actions. It highlights the need to educate children and the school community about the benefits and risks of using internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to control their online experience.

Our vision is, through collaboration with parents and carers, to ensure the children at Rose Hill Primary School are safe and productive in the online world, with particular focus on protection against grooming, cyberbullying and becoming a positive e-citizen.

Our policy and practice against this is clearly articulated in this online safety policy.

What is online safety?

Online safety is a school's ability to protect and educate a school's children and staff in their use of technology as well as having appropriate mechanisms in place to respond to, supporting any incident where appropriate.

a. Protect

Protecting children means providing a safe learning environment by using appropriate monitoring and filtering to control what children can access while at school. However, this only protects them while they are on school premises. Education around online safety is the only way to ensure that, wherever they are, they know how to stay safe online.

b. Educate

Learning about online safety is a vital life skill. Empowering children at an early age with the knowledge to safeguard themselves and their personal information is something that needs to be nurtured throughout school to see them into adult life. Equally it is important to empower adults, particularly parents, with the right information so that they can identify risky behaviour, mitigating the possibility of risk.

The School's online safety curriculum is progressive and covers a wide range of aspects, including:

- Online behaviour – understanding what constitutes cyber-bullying, inappropriate content and sexting, how to behave safely and with respect for others.
- Protecting your online reputation – understanding both the risks and rewards of sharing personal information online (your digital footprint).
- Learning to evaluate internet content – understanding how to research, evaluate and use published material

c. Respond

Responding to issues is both about ensuring children know what to do if anything happens to put their online safety at risk, taking direct and immediate action as a school where incidents occur.

Rose Hill Primary School has clear and robust policies and procedures to identify and immediately respond to online safety risks or incidents, efficiently and consistently. It is important to note that the school's remit to act goes beyond the classroom, to regulate children's conduct and safeguard them when they are not on school premises or under the lawful charge of school staff.

Why Use the internet for teaching and learning?

Many studies and government projects have identified the benefits to be gained through the appropriate use of the internet.

The rapid developments in electronic communications are having many effects on society. Only ten years ago we were asking whether the internet should be used in all schools. Now, it is an essential aspect of learning across all walks of life. In school, access to the internet is essential to:

- Raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

- Prepare children and young people for life in the 21st century in terms of education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience.
- Teach children how to evaluate internet information and to take care of their own safety and security rather than be sheltered from potential risks.

There are many benefits of the internet to learning:

- Access to world-wide educational resources
- Collaboration and communication between children
- Access to anytime, anywhere learning
- Educational and cultural exchanges between children world-wide to develop global understanding
- Access to experts in many fields for children and staff
- Professional development for staff through access to national developments, educational materials and example of 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 information

With increased use of the internet, protecting and educating children to manage the risk becomes our primary concern. As a school we commit to provide parents with support and information in keeping children safe online.

Policy

Cyber Bullying

Online bullying and harassment via instant messaging, mobile phone texting, email and chat rooms are potential problems that can have a serious effect on children both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and unintended involvement an increased risk. Rose Hill Primary School has a range of strategies and policies to prevent online bullying, outlined in various sections of this Policy. These include:

- A website filter that allows no access to public chat-rooms, Instant Messaging services and bulletin boards.
- Children are taught how to use the internet safely and responsibly and are given access to guidance and support resources from a variety of sources. Specific education and training on cyber bullying (understanding what behaviour constitutes cyberbullying and its impact, how to handle concerns and report incidents) is given as part of an annual Anti-Bullying Week and online safety Day.
- Children are encouraged to discuss any concerns or worries they have about online bullying and harassment with staff, who have a range of materials available to support children and their families.
- Children are informed on how to report cyberbullying both directly within the platform they are on, and to school.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.
- As a school, we develop skills using external agencies to ensure our understanding is up to date and reflective of changes in technology.

Grooming

Grooming is a word used to describe how people who want to co-opt or potentially harm children and young people get close to them, and often their families, and gain their trust. Online grooming may occur by people forming relationships with children and pretending to be their friend. They do this by finding out information and seeking to establish false trust. The school has measures in place to educate and protect children against this risk. These include:

- A website filter that ensures no access to public chat-rooms, Instant Messaging services and bulletin boards. No mobile phones are permitted to be used in school.
- All online access and child generated content in school is monitored and password protected.
- Children are taught how to behave responsibly online using the SMART Rules in protecting personal information.

- Children, staff, parents and governors are provided with appropriately targeted training on risks and solutions to keep safe online, including ongoing staff CPD from external agencies.

Authorising Internet Use

At Rose Hill Primary School pupil usage is supervised, with access to specific approved online materials. Children are authorised to access the internet as a group or independently, depending on the activity. All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resources, and parents are equally requested to share the Acceptable Use Policy with their children.

Managing Filtering

Whilst levels of internet access and supervision will vary according to the child's age and experience, our policy is that internet access must be appropriate for all members of the school community. Our internet connection was arranged by IT support company 123 ICT following advice from Oxfordshire County Council. Our Broadband is received by a dedicated internet connection and is tailored with filters to our specific needs. The procedures for ongoing management and review are:

- The school will work with Schools Broadband and 123 ICT to ensure that systems are reviewed, and any improvements are implemented.
- If staff or children discover unsuitable sites, the URL must be reported to a member of the 123ICT team who will then ensure that the URL is blocked.
- Any material that the school believes to be illegal must be reported to appropriate agencies (IWF or CEOP)

Managing Email and Communications

Email is an essential means of communication for both staff and children. Directed email use can bring significant educational benefits.

All staff are given a secure school email address upon joining the school. The creation of these accounts is the responsibility of the school's Business Manager. Should any staff need to contact parents directly then they should use their school email, or if relevant, through ParentMail, otherwise all communications should be passed on by the school office. All personal contact details for staff members will remain private.

Children are not provided with a school email account.

Managing Published Content and Images

Our school website and social media celebrates children' work, promotes the school, publishes resources and acts as a communication tool. Publication of information on the Rose Hill Primary School website is carefully considered from a personal and school security viewpoint.

Contact details available on the website are school address, email and telephone number. Staff or children's personal information must not be published, and all images used will comply with our data protection policy.

Managing Information Services

Rose Hill Primary School commits to take due care regarding managing the provision of Information Services to support secure and appropriate access. The measures outlined in this Policy include:

- The security of the school information system is reviewed regularly 123 ICT.
- The school keeps the network secure with several group policy settings and permissions which only allow certain users to use portable storage devices and to access and open certain drives and files.
- The school reserves the right to monitor user areas and equipment provided by the school.
- Sophos anti-virus software updates automatically every hour. Staff are also encouraged to install Sophos at home to increase security.
- The school uses an internet firewall and filters are provided

Social Networking and Personal Publishing

Parents and teachers need to be aware that the internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. There is increasing educational potential of such tools, for example in the use of blogs and wikis to improve writing.

However, whilst direct access to social networking sites in school is limited and regulated, a significant number of children in upper KS2 now use social networking out of school hours on a regular basis. As a school, we recognise that they may need guidance and support in knowing how to stay safe in such sites, and parents may not know what advice to give them. Children need to be encouraged to consider the implications of uploading personal information and the relative ease of adding the information and the practical impossibility of removing it.

Children need to be taught the reasons for caution in publishing personal information and photographs on the internet and on social networking sites. Our online safety Policy aims to provide guidance and council on keeping safe within social networking and personal publishing. Specific council is:

- Children are advised to never give out personal details of any kind, which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended,
- Children are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Staff must ensure their profiles on social networking sites are private and not to add past or present children as friends.
- Staff should not give out their personal email address to parents. All communications must go through the school office.
- Staff and children are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children are encouraged to invite known friends only and deny access to others. They are advised not to publish specific and detailed private thoughts.
- Parents and carers are advised to ensure that their children's social media accounts are set up with security features, such as private modes, to help support their safety online.
- Staff, parents and carers need to be aware of and follow the school's code of conduct and acceptable use policy when using social media linked to and relative to the school.

We very much acknowledge that we cannot act in isolation and parent's co-operation in supporting these steps is greatly appreciated.

Guidelines by Technology

The Policy is applied across a range of technologies that continue to expand and evolve. In addition to computers and tablet devices commonly used to access the internet or enable communications, this Policy outlines clear guidelines as they apply to other known and used technologies. Specifically:

Video Conferencing

Video conferencing, including Skype and FaceTime, enables users to see and hear each other between different locations. It is a 'real time' interactive technology and has many uses in education. The practices below aim to ensure that we apply our online safety commitments to video conferencing.

Equipment:

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- IP video conferencing must use the educational broadband network to ensure quality of service and security rather than the internet.
- Video conferencing contact information will not be put on the school website
- The equipment must be secure and locked away when not in use.

Users:

- Video conferencing will be supervised by an appropriate adult at all times.
- Children must ask permission from the teacher before making or answering a video conference call.

Content:

- When a lesson is to be recorded, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of video conference must be clear to all parties at the start of the conference.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, checks will be made to ensure that they are delivering material that is appropriate for the audience.

Internet enabled mobile phones and handheld devices

Increasingly, a greater number of young people have access to new and sophisticated internet-enabled devices such as smart phones, tablets and music players. It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the internet, and allow pictures and information to be remotely posted to a website or weblog.

Our policy is that children are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for children who may need them on their journey to and from school.

However, in acknowledgement of the growing use, children will be taught about the benefits and risks, the legal and moral implications of posting photos and personal information from mobile phones to public websites, and how the data protection and privacy laws apply.

Online Gaming

Online gaming can be a helpful and engaging way of developing learning through play with a range of educational content presented through games to support literacy, maths, problem solving, strategy or coding. Controlled use may be supported within the classroom but always through screened individual log-in programs or via teacher lead activity where fit for use and appropriate access settings have been pre-assessed.

However, we also recognise from our recent internet Survey that gaming plays a key part in recreational play in the home setting or when with friends. We have therefore outlined some best practice guidance from Microsoft which will help to support and keep children safe when gaming online.

Making safe choices:

All games all have age guidance ratings so that content can be assessed as appropriate. Check the ratings of the games your children want to play. In the UK most games for consoles or online have a PEGI rating which can be found on pack or searched for via the PEGI website. You can use these ratings as you discuss the most appropriate games with your child. In line with our safeguarding policy we would look to protect children from content that is violent or inappropriate by advising strongly that children are not permitted access to games with a PEGI rating greater than 7.

Beyond the content rating, selecting games that are well-known or those from reputable sites will reduce the risk of downloading viruses or sharing data in an unprotected way. You can also review the game's terms of play to find out how the game service monitors players and respond to abuse and read the site's privacy policy to learn how it will use and protect children's information.

Being aware of the risks:

Games that have no online connection, no entry of personal data or passwords and that are user only controlled do not pose a potential online safety risk, however, to add an extra dimension to a game there is increasingly a multiplayer element, where players often communicate via integrated chat or verbally with microphone or a headset.

Many games – from simple chess to first-person adventure games, where thousands of players participate at the same time – include these features. The presence of such a large online community of anonymous strangers and the unfiltered, unmoderated discussions, can pose a variety of potential risks such as:

- Inadvertently giving away personal information, including password, email or home address or age.
- Inappropriate contact or behaviour from other gamers
- Buying or selling virtual, in-game property – for example high-level characters – where there is real money involved.
- Disposing of game consoles, PCs and mobile devices without deleting your personal information and account details.
- Playing games for many hours at a time with the danger of becoming addicted.

Recommended solutions:

- Gaming can be an enriching learning experience with some simple steps to keep safe:
- Play online games only when you have effective and updated antivirus software and firewall running.
- Play only with authorised versions of games which you have purchased from the correct sources and for which you have a licence. Verify the authenticity and security of downloaded files and new software by buying from reputable sources.

- Choose a username and password with your child that does not reveal personal information. Similarly, if the game includes the ability to create a personal profile, or where contact can be made by other players make sure that no personal information is given away.
- Read the manufacturer or hosting company's terms and conditions to make sure there will not be any immediate or future hidden charges.
- When disposing of your gaming device either by selling, scrapping, giving away or donating, ensure all your personal information and your account details have been deleted.
- Set guidelines and ground rules for your children when playing online. This could include time limitations, parent entered passwords or game play only in communal areas

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. A risk assessment needs to be undertaken on each new technology, and effective practice in the classroom should be developed. The contents of this policy are regularly reviewed and updated considering the on-going changes to modern technologies.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protective Behaviour

A critical part of our online safety Policy which applies across all technologies are the behaviours we seek to embed, and as a school, being proactive in ensuring that actions are put in place to keep children safe.

<table>
<tr><th colspan="2">Behaviours</th></tr>
<tr><td>Personal Information is Personal

Children learn to never give out personal details such as name, address, date of birth and school. Usernames and passwords should not contain personal information</td><td>Treat Others Online as You Would in the Real World

Children learn that online bullying and harassment are potential problems that can have a serious effect on children. They are aware that causing upset or harm online will follow the same actions as outlined in our behaviour and relationships policy.</td></tr>
<tr><td>Strangers Online Are Still Strangers

Children learn that friends are people we know and see regularly as part of our everyday lives. Online ‘friends’ are strangers and invitations to meet them in the real world should be reported</td><td>Evaluate What You See and Do

Children learn to evaluate everything they read and to refine their own publishing and communications with others via the internet. They are supported in learning to evaluate internet content.</td></tr>
<tr><td colspan="2">What to Do If Something Isn’t Right

Children learn that if they know or feel something isn’t right that they should speak to or contact someone they trust immediately.</td></tr>
</table>

Actions

The school would take immediate action if children or staff were to put themselves or others at risk. There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.

Children: Actions within the school’s Behaviour and Relationships Policy will apply.

Staff: It is essential for staff to use the internet, including social media in a responsible and professional manner both in school and out of school, to ensure the privacy and safety of all employees, children, parents and members of the wider school community.

Incidents relating to irresponsible internet use will be brought to the employee’s attention as soon as possible to resolve the situation informally, however if appropriate more formal procedures will be set in motion in-line with OCC and Academy guidance.

Handling Online Safety Complaints

Complaints of online misuse by staff will be initially dealt with by the headteacher in accordance with the staff allegation policy and if necessary escalated to the local authority designated officer (LADO).

Complaints of online misuse by children will be dealt with by the class teacher, headteacher or SLT, and if appropriate, advice would be sought from the local authority in accordance with our child protection policy.

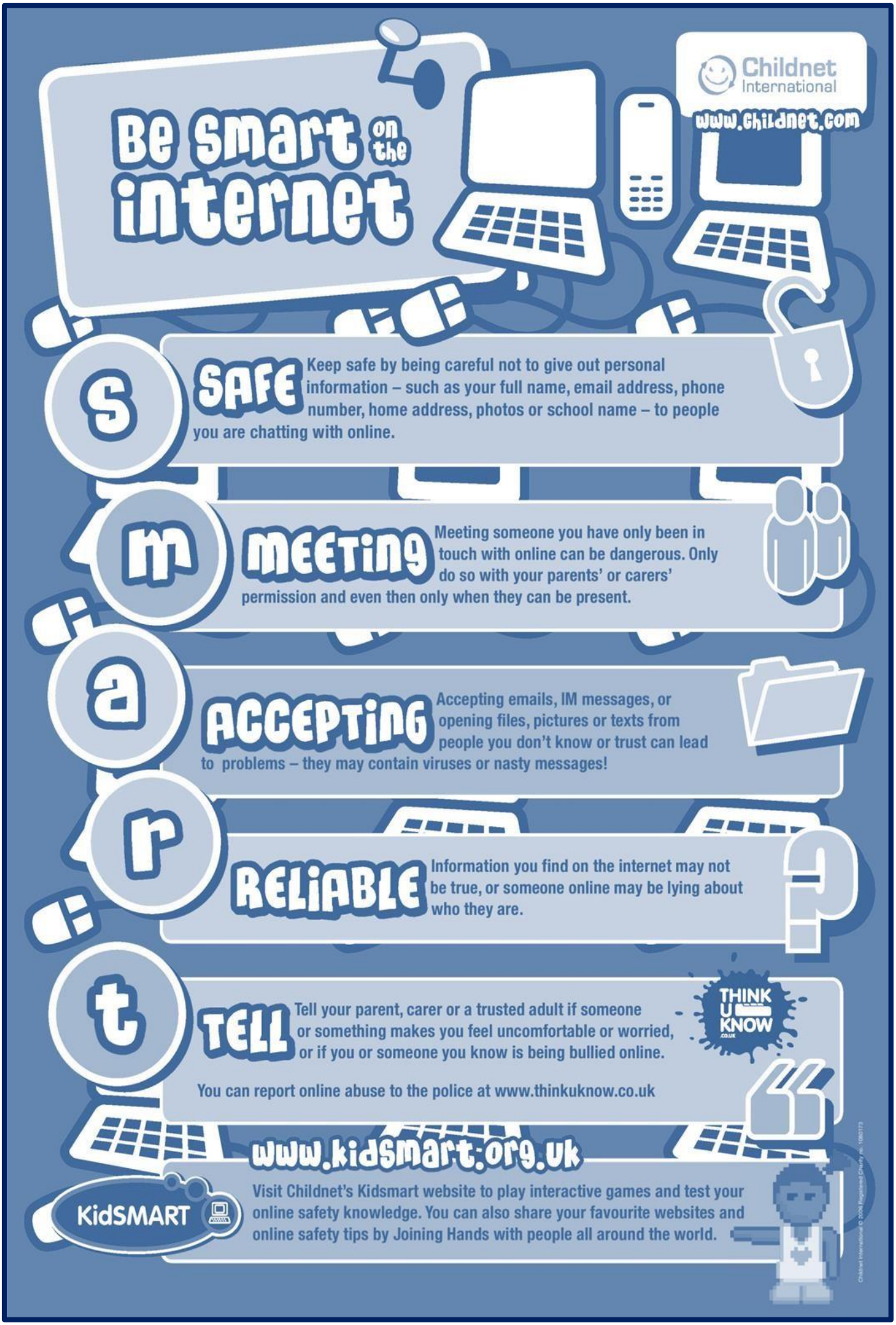
Learning to Evaluate Internet Content

Developing best practice internet use is imperative. Parents and teachers can help children learn how to distil the meaning from the mass of information provided on the internet.

Often the quantity of information is overwhelming and staff guide children to appropriate websites or teach search skills. Information received via the internet, email, or text message requires good information handling skills. Our approach is to offer younger children a few good sites as this is often more effective than an internet search. Respect for copyright and intellectual property rights, and the correct use of published material are taught.

Above all children need to learn to evaluate everything they read and to refine their own publishing and communications with others via the internet. Specifically:

- The school internet access is designed expressly for child use and includes filtering appropriate to the age of children.
- Children are taught what internet use is acceptable and what is not and are given clear objectives for internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide children in online activities that support the learning outcomes planned for the children's age and maturity.
- Computing skills lessons are used to educate children in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. This is reinforced by teachers when using the internet within their classroom.
- The school ensures that copying and subsequent use of the internet derived materials by staff and children complies with copyright law.
- Children are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.


Childnet International
www.childnet.com
Be smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
M
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
A
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
R
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
T
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
THINK U KNOW .co.uk
You can report online abuse to the police at www.thinkuknow.co.uk
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Online Safety Contacts and References

Childnet International	http://www.childnet.com/resources
Childline	http://www.childline.org.uk
Think U Know (links to CEOP)	www.thinkuknow.co.uk
Child Exploitation and Online Protection Centre	www.ceop.gov.uk
Stop It Now (child sexual abuse prevention campaign, for all adults)	www.stopitnow.org.uk
Parents Protect	www.parentsprotect.co.uk
online safety self-review tools provided by **South West Grid for Learning**	www.360safe.org.uk
Securus (Company supplying software to protect children from cyberbullying in schools)	www.securus-software.com
Internet Watch Foundation (IWF) – website for the public to report potentially illegal online content	www.iwf.org.uk
CBBC Stay Safe	www.bbc.co.uk/cbbc/topics/stay-safe
BBC Chat Guide	http://www.bbc.co.uk/chatguide/
Becta	http://www.becta.org.uk/schools/esafety
online safety in Schools	http://www.kenttrustweb.org.uk?esafety
Grid Club and the **Cyber Cafe**	http://www.gridclub.com
Internet Safety Zone	http://www.internetsafetyzone.com/
Kent Primary Advisory online safety Pages	http://www.kented.org.uk/ngfl/ict/safety.htm
Kidsmart	http://www.kidsmart.org.uk/
NCH – The Children's Charity	http://www.nch.org.uk
NSPCC	http://www.nspcc.org.uk
Schools online safety Blog	http://clusterweb.org.uk?esafetyblog
Schools ICT Security Policy	http://www.eiskent.co.uk
Oxfordshire County Council website – for child safeguarding concern	http://www.oxfordshire.gov.uk/cms/public-site/child-social-care
CEOP – report a child in danger of abuse. Children can self-report.	http://www.ceop.police.uk/safety-centre/

ANNEX 1:

The extract below has been taken from the Covid-19 updated Safeguarding Policy that has been produced by the Education Safeguarding Advisory Team.

Children and online safety away from school and college

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Rose Hill Primary School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- *Staff and children must wear suitable clothing, as should anyone else in the household.*
- *Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.*
- *The live class should be recorded so that if any issues were to arise, the video can be reviewed.*
- *Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.*
- *Language must be professional and appropriate, including any family members in the background.*
- *Staff must only use platforms provided by Rose Hill Primary School to communicate with pupils*
- *Staff should record, the length, time, date and attendance of any sessions held.*

All staff at Rose Hill Primary School will be reminded of the following policies:

- *Staff code of conduct*
- *Acceptable users' policy*
- *Social media guidance*

Additional considerations:

Practice Considerations for Staff members

- Teachers and support staff should continue only to use school approved methods to communicate with pupils.
- Communications to take place during school hours.
- As per the ICT Acceptable Use Policy, staff should not use their private email addresses, WhatsApp groups or any other form of social media that is not directly regulated by the School to communicate with pupils.
- When communicating individually with pupils, staff should email via their school email address only and should copy in other pastoral staff (*e.g.* tutor, Housemaster) when necessary.
- Staff should make the agreed person (head for example) aware of when they will be using the school agreed platform (Teams for example).
- Staff members should avoid live 1:1 audio or video contact with individual pupils both to safeguard pupils and to safeguard themselves. If 1:1 contact cannot be avoided, permission to be gained from head/manager.
- Colleagues should use the school approved platform to upload pre-recorded video clips that they have made.
- In any recorded video, staff should ensure that no personal identifying information can be seen in the background. Dress should be appropriate, and the background should be appropriate and not contain any personal information.
- In all video footage recorded by teachers, people who are not connected to the school should not appear.

Practice considerations for live-streaming of audio and visual content

- Staff should only use school provided equipment for live-streaming sessions.
- Staff should record live sessions, where possible, and store them in the relevant class area of the school approved platform both for safeguarding reasons and to share with pupils who cannot access the session at the time. It is imperative to make sure that all participants are aware of this.
- At the start and throughout sessions, teachers should be clear about the expectations of student behaviour (*e.g.* a 'classroom standard' of behaviour is expected from all participants and they should usually mute their microphones unless they want to ask a question). Be clear that neither the recording by pupils nor the onward sharing of events is acceptable.
- Staff should make a note of the conference timing and who participated, including those that arrived/departed early or late.

Considerations for one to one lesson's (peripatetic music teachers for example)

- When using live video streaming facilities for one-to-one lessons, a responsible adult is always present to accompany the pupil for the lesson. The responsible adult must answer each call to show that they give their consent for the lesson to take place. They must then either remain in the room or nearby for the duration of the lesson, to ensure adequate supervision. No other children should be present, and teachers must end a lesson if there are other children visible
- Before online lessons can commence, parents/carers must give their consent in writing that they are happy for their child to receive online tuition, that they are aware that lessons will be recorded and that they give their consent for this.
- Teachers should only use school/organisation provided equipment for live-streaming sessions.
- Teachers should where possible record live sessions and store them in the agreed area (as detailed in school policy). The responsible adult and student should be made aware that this is happening.

Useful links for further guidance/support

The links below are not endorsed by ESAT and have been added as a resource for settings/schools to gain further information.

https://support.safeguardinginschools.co.uk/article/36-why-schools-shouldnt-use-whatsapp
https://coronavirus.lgfl.net/safeguarding
https://support.safeguardinginschools.co.uk/article/37-remote-teaching-and-learning-during-the-coronavirus-outbreak
https://swgfl.org.uk/resources/safe-remote-learning/