



Brookhurst Primary School
Digital Safety Policy
September 2022

Background and Rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Child on child abuse
- Sexting
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Policy and Leadership

Responsibilities: E-safety coordinator

Our e-safety coordinators April Parsonage is the person responsible to the Headteacher and Governors for the day to day issues relating to e-safety. The e-safety coordinator:

- lead the e-safety committee as well as discussions on e-safety with the Pupil Parliament
- take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provide updates and advice for staff
- liaise with the Local Authority and other schools
- liaise with school ICT technical staff
- monitor reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- meets with safeguarding governor to discuss current issues, review incident logs and filtering change control logs

Responsibilities: Governors

Our Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

- monitoring of e-safety incident logs
- reporting to relevant Governor committee meetings

Responsibilities: Headteacher

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the e-safety coordinators
- The Headteacher and other members of the senior management team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. See flow chart on dealing with e-safety incidents – below and relevant Local Authority HR / disciplinary procedures)

Responsibilities: Classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school's Acceptable Use Policy for staff
- they report any suspected misuse or problem to the e-safety coordinators
- digital communications with students (email / Google Classroom/ voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in the curriculum and other school activities.

Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are reported to the ICT coordinator or Headteacher so that appropriate action may be taken.

Policy Development, Monitoring and Review

This e-safety policy had been agreed by:

- School e-safety coordinator
- Headteacher/Senior Leadership Team
- Teachers and TAs
- ICT Technical staff
- Governors (especially the e-safety governor)
- Pupils

Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers the Headteacher, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that takes place out of school.

Acceptable Use Policies

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable use policies are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers (including permissions to use pupil images/work and to use ICT systems)

Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents.

For children in EYFS and KS1 parents may sign on behalf of their children

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the schools ICT resources (including the internet) and permission to publish their work.

Other policies relating to e-safety

ICT Policy How ICT is used, managed, resourced and supported in our school

PSHE E-Safety has links to this – staying safe

Safeguarding Safeguarding children electronically is an important aspect of e-safety. The e-safety policy forms a part of the school's safeguarding policy

Behaviour Linking to positive strategies for encouraging e-safety and sanctions for disregarding it.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (**those in bold are illegal**) and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial, religious hatred or radicalisation
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on ICT kit provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Wirral Council and/or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial/ personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- Use of personal social networking sites/profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupil Sanctions

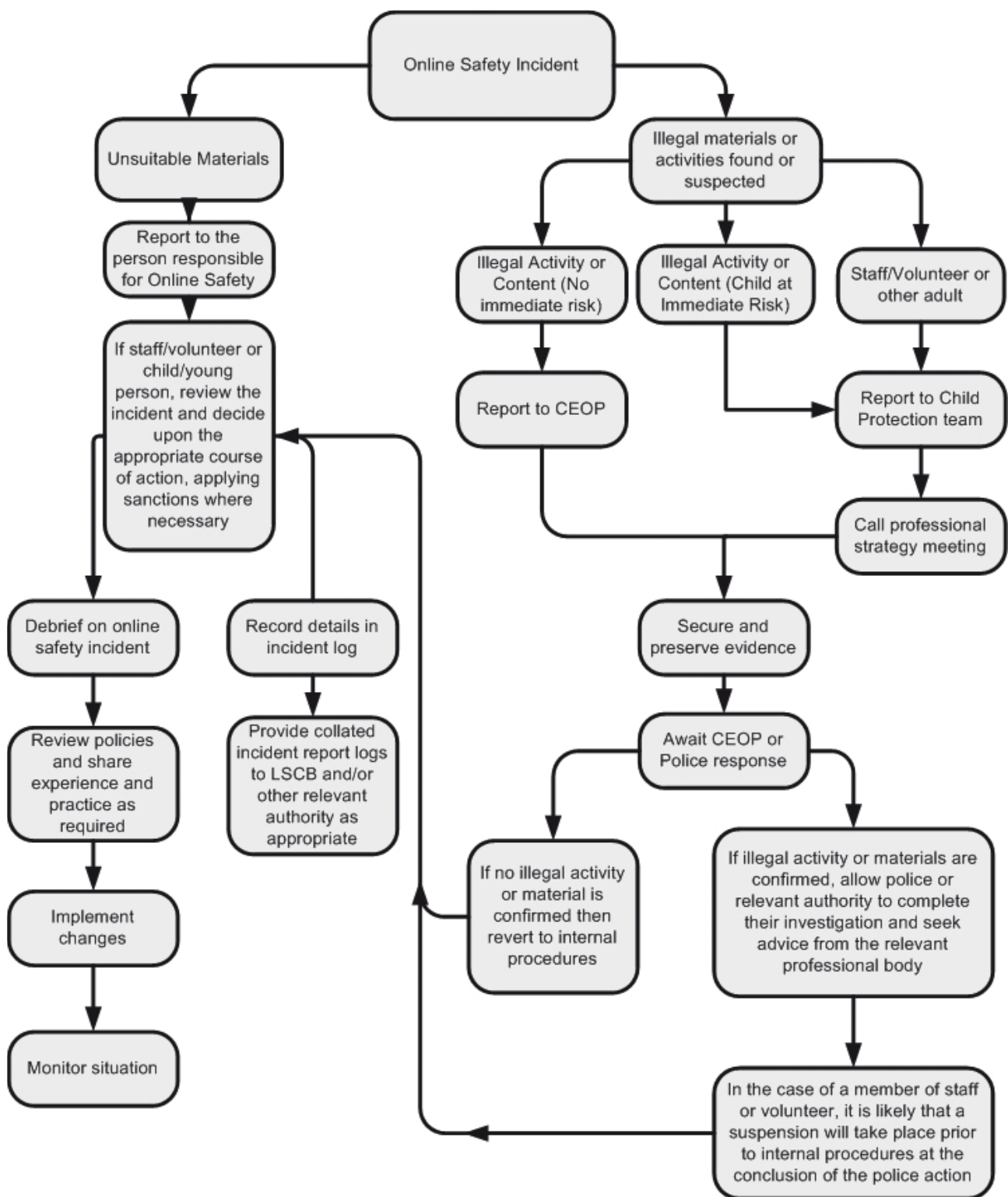
	Refer to class teacher	Refer to e-safety coordinator	Refer to Headteacher	Refer to Police	Refer to e-safety coordinator for action re filtering security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. time out / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unauthorised use of non-educational sites during lessons	<input type="checkbox"/>				<input type="checkbox"/>		<input type="checkbox"/>		
Unauthorised use of mobile phone / digital camera / other handheld device	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>			
Unauthorised use of social networking / instant messaging / personal email	<input type="checkbox"/>				<input type="checkbox"/>				
Unauthorised downloading or uploading of files	<input type="checkbox"/>				<input type="checkbox"/>				
Allowing others to access school network by sharing username and passwords	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		
Attempting to access the school network, using another pupil's account	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		
Attempting to access or accessing the school network, using the account of a member of staff	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>		
Corrupting or destroying the data of other users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>		<input type="checkbox"/>	
Continued infringements of the above, following previous warnings or sanctions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>		<input type="checkbox"/>	
Using proxy sites or other means to subvert the school's filtering system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	
Accidentally accessing offensive or pornographic material and failing to report the incident	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>			
Deliberately accessing or trying to access offensive or pornographic material	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Staff Sanctions

	Refer to Key Stage Leader	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>		
Unauthorised downloading or uploading of files	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>		
Careless use of personal data eg holding or transferring data in an insecure manner	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>		
Deliberate actions to breach data protection or network security rules	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>		
Actions which could compromise the staff member's professional standing	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>		
Using proxy sites or other means to subvert the school's filtering system	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Accidentally accessing offensive or pornographic material and failing to report the incident	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>		
Deliberately accessing or trying to access offensive or pornographic material	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Breaching copyright or licensing regulations	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>		
Continued infringements of the above, following previous warnings or sanctions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:



Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them.

Broadly speaking this is:

- Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
- Members of staff are free to use these devices in school, outside directed work time.
- Y5 and 6 pupils who walk home from school on their own are permitted on receipt of written permission from parents to bring their mobile phones into school. These must be handed in to the class teacher on entry into school and collected at home time. Pupils are not allowed to use their phones on school premises.

Email


Access to email is provided for all staff in school via Gmail. These official school email services may be regarded as safe and secure and are monitored.

- Confidential emails which are not linked to Gmail can only be sent by the Headteacher and Deputy Headteacher using VIRTRU encryption.
- Users need to be aware that email communications may be monitored.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (these may be blocked by filtering).
- Users must immediately report, to their class teacher/e-safety coordinators – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

Use of web-based publication tools

Our school uses the public website, www.brookhurst.wirral.sch.uk for sharing statutory information with the community beyond our school. We also maintain the public face of the school on acebook. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content. We also use Tapestry in the infants.

- Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
- Only pupil's first names are used on the website, and only then when necessary.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
 - pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
 - Permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the **Teachers' Standards** as described by the DfE (<http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf>). Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

- These communications should only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat/social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from Hi-impact Services we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **e-safety coordinators** (with ultimate responsibility resting with the **Headteacher and Governors**). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the filtering service must:

- be logged in a change log
- be authorised by a second responsible person prior to changes being made (this will normally happen anyway, as part of the process and will be the class teacher who originally made the request for the change).

All users have a responsibility to report immediately to class teachers/e-safety coordinators any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education/Training/Awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (a part of their induction process)
- briefing in staff meetings, training days, memos etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions/newsletter etc.

Monitoring

- No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

Audit/Reporting

Logs of filtering change controls and of filtering incidents are made available to

- the safeguarding governor
- *the e-safety committee*

This filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

E-safety Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- We use a range of resources for teaching internet safety, including the following:
<http://www.thinkuknow.co.uk/teachers/resources/>
Google “Be Internet Legends” (KS2)
1decision (school online PSHE scheme)
Hi Impact lesson plans
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT both within and outside school. As a school we realise that some pupils will engage in risky or unacceptable behaviour online in spite of all efforts to educate them in safety. Where we are made aware that this has occurred we will inform parents and seek to support and reiterate safety messages in school through class or individual discussions (but see pupil sanctions chart on page 8). There is some Safer Internet Guidance which has been agreed with staff, pupils and parents (see appendix 2)
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils are not allowed to freely search the internet, e.g. using search engines: staff should monitor the content of any websites intended for us within the classroom before sharing with pupils.

Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
 - Checking the likely validity of the URL (web address)
 - Cross checking references (can they find the same information on other sites)
 - Checking the pedigree of the compilers/owners of the website
 - See lesson 5 of the Cyber Café Think U Know materials below
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require

The contribution of the children to e-learning strategy

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

Pupils play a part in monitoring this policy.

Staff training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The E-Safety Coordinators will receive regular updates through attendance at local authority or other information/training sessions and by reviewing guidance documents released by the DfE or local authority.
- All teaching staff have been read this e-safety policy and are therefore aware of its content.
- The e-safety coordinators will provide advice, guidance and training as required to individuals as required on an on-going basis.

Governor Training

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee or group involved in ICT, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or by the National Governors Association or other bodies.
- Participation in school training/information sessions for staff or parents

The e-safety governor works closely with the e-safety coordinators and reports back to the full governing body .

Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, workshops, parent emails, Facebook
- Parents evenings
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others

Remote /blended learning as a result of the Covid-19 Pandemic – See Appendix 3

Appendix 1

Acceptable use Policy Agreements

Acceptable Use Policy Agreement – pupils (KS1)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- I will only use activities that an adult says are OK.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them.

My name:		Date
R - Signed (child):		
Y1 - Signed (child):		
Y2- Signed (child):		

Acceptable Use Policy Agreement – pupils (KS2)

I understand that while I am a member of Brookhurst Primary School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will, wherever possible be supervised and monitored.
- I understand that my use of the internet will be monitored
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal ICT kit if I have permission and then I will use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes on ICT devices belonging to the school unless I have permission.
- I will only use social networking, gaming and chat through the sites the school allows.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:		Date
Y3: Signed		
Y4: Signed		
Y5: Signed		
Y6: Signed		

Acceptable Use Policy Agreement – Staff & Volunteer

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the e-safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the e-safety policy and then in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems except in an emergency
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies (see e-security policy).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not use my own mobile device during directed 'work' or teaching time unless approval has been agreed by the SLT.

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff/ Volunteer Name:	
Signed:	
Date:	

Acceptable Use Policy Agreement and Permission Forms

– Parent/Carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times. This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using ICT (especially the internet).
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Child's name	
Parent's name	
Parent's signature:	
Date:	

Permission for my child to use the internet and electronic communication

As the parent/carers of the above pupil(s), I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Parent's signature:	
Date:	

Permission to use digital images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by name.

As the parent/carer of the above pupil, I agree to the school taking and using digital images of my child(ren). I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at school events, where permitted, which include images of children I will abide by these guidelines in my use of these images.

Parent's signature:	
Date:	

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the school website and in the school's virtual learning environment (VLE)

As the parent/carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

Your agreement of consent will carry through the school. If your circumstances change it is your responsibility to inform the school.

Our school's e-safety Policy, which contains this Acceptable Use Policy Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Acceptable Use Policy Agreement – Community User

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to agree to this acceptable use policy.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT system being withdrawn.

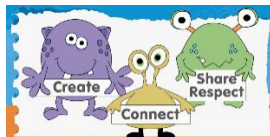
Community user Name:		
Signed:		Date:

Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- Have more than one senior member of staff/ volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of ‘grooming’ behaviour
 - the sending of obscene materials to a child
 - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.



BROOKHURST PRIMARY SCHOOL

SAFER INTERNET GUIDANCE

This guidance has been devised by children, staff, parents and governors of our school.

- Set appropriate security levels on all internet platforms
- Limit your child's device/phone time during the week to one hour per day.
- Stop all screen time one hour before the children go to sleep
- Remove devices from bedrooms before bedtime.
- *Ideally we would ask that you don't allow your child access to social media sites which have age restrictions above their chronological age. However, if you do:*
- Don't share anyone's contact details without their permission
- Don't add anyone into a group chat without their permission
- Don't remove anyone from the group (unless they have said something inappropriate)
- If someone leaves a chat, respect their decision
- Don't make inappropriate personal comments to someone or about someone
- If you are upset or cross, wait until you can talk about it face-to-face
- Don't forward chain messages or upsetting content
- Don't share photos of anyone without their permission
- Don't pester people to respond
- Don't send messages or posts at night

Appendix 3

Remote learning as a result of Covid-19

Guidance

Safeguarding and remote education during coronavirus (COVID-19)

Understand how to follow safeguarding procedures when planning remote education strategies and teaching remotely during the coronavirus (COVID-19) outbreak.

Published 19 April 2020

Last updated 6 October

From: [Department for Education](#)

Applies to:

England

Contents

1. [Safeguarding pupils and teachers online](#)
2. [Reporting concerns](#)
3. [Communicating with parents, carers and pupils](#)
4. [Virtual lessons and live streaming](#)
5. [Providing pastoral care remotely](#)
6. [Personal data and GDPR](#)

The latest update includes:

- reference to local restrictions
- links to new resources

This guidance is to help schools and teachers support pupils' remote education during the coronavirus (COVID-19) outbreak. It should be read alongside statutory safeguarding guidance on [keeping children safe in education](#).

Where a class, group or small number of pupils need to self-isolate, or there are local restrictions requiring pupils to remain at home, the Department for Education expects schools to be able to immediately offer them access to remote education. Schools should ensure remote education, where needed, is safe, high quality and aligns as closely as possible with in-school provision.

Schools should continue to improve the quality of their remote education and have a strong contingency plan in place for remote provision.

Safeguarding pupils and teachers online

Keeping pupils and teachers safe during remote education is essential. Teachers delivering remote education online should be aware that the same principles set out in the school's staff behaviour policy (sometimes known as a code of conduct) will apply.

Schools may wish to use these resources to understand more about how to ensure online education is safe:

- remote education advice from [The Key for School Leaders](#)
- advice from [NSPCC](#) on undertaking remote education safely
- guidance from the [UK Safer Internet Centre](#) on remote education

Schools can access the free [Professionals Online Safety Helpline](#) which supports the online safeguarding of both children and professionals. Call 0344 381 4772 or email helpline@saferinternet.org.uk. The helpline is open from Monday to Friday from 10am to 4pm.

Guidance on [teaching online safety in schools](#) provides information to help schools ensure their pupils understand how to stay safe and behave online.

School contact with parents and carers during this time can also be used to reinforce the importance of children staying safe online.

It is especially important for parents and carers to be aware of what their children are being asked to do, including:

- sites they will be asked to use
- school staff their child will interact with

Schools should emphasise the importance of a safe online environment and encourage parents and carers to set age-appropriate parental controls on digital devices and use internet filters to block malicious websites. These are usually free, but often need to be turned on.

Use these resources to support parents and carers to keep their children safe online:

- [support for parents and carers to keep children safe online](#), which outlines resources to help keep children safe from different risks online and where to go to find support and advice
- guidance on [staying safe online](#) which includes information on security and privacy settings
- [Thinkuknow](#) provides advice from the National Crime Agency (NCA) on staying safe online
- [Parent info](#) is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations
- [Childnet](#) offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- [Internet matters](#) provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- [London Grid for Learning](#) has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- [Net-aware](#) has support for parents and carers from the NSPCC, including a guide to social networks, apps and games
- [Let's Talk About It](#) has advice for parents and carers to keep children safe from online radicalisation
- [UK Safer Internet Centre](#) has tips, advice, guides and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services

Reporting concerns

It is essential to have and communicate clear reporting routes so that children, teachers, parents and carers can raise any safeguarding concerns in relation to remote online education.

Schools may wish to review the existing arrangements (including their child protection policy) to ensure they are appropriate and reflect remote online education, or whether additional or alternative arrangements need to be put in place.

Schools should consider referring teachers, parents and carers to the practical support that's available for reporting harmful or upsetting content as well as bullying and online abuse.

Harmful or upsetting content

Get support by:

- reporting harmful online content to the [UK Safer Internet Centre](#)
- getting government advice and trusted resources from [Educate Against Hate](#) on safeguarding from radicalisation, building resilience to extremism, and promoting shared values

Bullying or abuse online

You can:

- get advice on reporting online abuse from the National Crime Agency's [Child Exploitation and Online Protection command](#)
- get advice and support from [Anti-Bullying Alliance](#) for children who are being bullied

Schools may also wish to use resources such as [Tootoot](#) to provide a confidential route for pupils to report bullying or abuse.

Communicating with parents, carers and pupils

Where education is having to take place remotely due to coronavirus (COVID-19), it's important for schools, teachers and pupils to maintain professional practice as much as possible. When communicating online with parents and pupils, schools should:

- communicate within school hours as much as possible (or hours agreed with the school to suit the needs of staff)
- communicate through the school channels approved by the senior leadership team
- use school email accounts (not personal ones)
- use school devices over personal devices wherever possible
- advise teachers not to share personal information

Virtual lessons and live streaming

Should we choose to provide remote education using live streaming or pre-recorded videos, we will use Google Meet, using [guidance from the UK Safer Internet Centre on safe remote learning](#) which includes detailed advice on live, online teaching.

Teaching from home is different from teaching in the classroom. Teachers should try to find a quiet or private room or area to talk to pupils, parents or carers. When broadcasting a lesson or making a recording, consider what will be in the background.

Providing pastoral care remotely

Where pupils are required to remain at home (for example, if pupils need to self-isolate or there are local restrictions) helping parents, carers and pupils to make a weekly plan or structure is important. These plans should include time for education, playing and relaxing to reduce stress and anxiety.

As set out in [Public Health England's guidance for parents and carers](#), routine can give children and young people an increased feeling of safety in the context of uncertainty.

Schools might want to consider whether one-to-one sessions could be appropriate in some circumstances. For example, to provide pastoral care or provide support for pupils with special educational needs and disabilities (SEND).

This should be discussed and approved by the senior leadership team to assess any risks. There may be helpful solutions, such as including a parent or additional staff member in the call.

Personal data and GDPR

Schools should continue to follow the guidance outlined in the [data protection: toolkit for schools](#) when managing personal data and may need to consider:

- taking care not to share contact details when emailing multiple people
- being careful when sharing usernames and other personal data for access to online resources
- providing access to school data systems safely



BROOKHURST PRIMARY SCHOOL

Video Conferencing: Safeguarding and Privacy Overview



Google Meet / Hangout



Summary privacy policy (Powered by Polisis)

✓ Positive

- The policy offers you clear links to control your data
- You can request access and deletion of personal data
- The policy provides opt-out choices

— What to look out for

- Several types of personal information types can be collected.
- Personal information may be shared with third parties for marketing/advertising reasons.
- Some data might be retained indefinitely.

[Read the full summary on Polisis.](#)

Personal data policy statements (adherence to GDPR/Privacy Shield)

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

We provide the controls described in this policy so you can exercise your right to request access to, update, remove, and restrict the processing of your information. You also have the right to object to the processing of your information or export your information to another service.

GDPR compliance - <https://privacy.google.com/businesses/compliance/>

How children's data is managed

No particular reference to management of children's data.

Minimum Age: Not available

- Pricing (per month) -
included within G Suite
- G Suite for Education - Free
- G Suite Enterprise for Education - \$48/user/year

Note: Google have extended their premium features to all G Suite customers until 30 September 2020. This means a larger numbers of participants can connect at the same time (250 vs 100). G Suite Enterprise is available at a promotional price until 31 July 2020, students are free.

Links

Terms and privacy -
<https://policies.google.com/>



BROOKHURST PRIMARY SCHOOL

Safe Remote Learning

The Covid-19 outbreak may mean enforced school closure becomes more likely. Take the opportunity to plan before you close (enforced or autonomously) and carefully consider how to safeguard your remote learning

There are a number of online options that schools may consider, ranging from merely setting homework or providing access to online resources through video tutorials and interactive video conferencing. Staff capability and the age of your children is going to determine your approach.

Whilst there are no expectations for you to do so, if you do decide to use audio and video for real-time online teaching, here are some things you might want to consider to help safeguard staff and children:

Organisation

- Do school online safety policies (Acceptable Use / Safeguarding / Standards) reference online teaching?
- How will personal data be managed?
- Have staff access to school systems and data?
- How will safeguarding be managed and have staff been trained?
- Consider the location children join from and what can be seen and heard on screen.

Participation

- Whilst clearly determined by age, setting tasks may be more manageable than timetabling lessons online
- How will children be supervised and what are the expectations of participation and attendance?
- What work will children be expected to do and when?
- How will parents be contacted and involved?

Technology

- Do staff and children have the necessary technology and access?
- Who will provide technical support?
- How will classes be conducted online, using what service / platform / tools / features?
- Have the technology service terms and privacy statements been considered?

Always follow local guidelines for recording video conferences

swgfl.org.uk/saferemotelearning



If you have questions or concerns then contact the Professionals Online Safety Helpline on 0344 381 4772 or email at helpline@saferinternet.org.uk



Remote Working

a guide for education professionals

It is likely that COVID-19 restrictions will continue for some time. There is a growing sense of mis-information about what is and isn't good practice around safeguarding students who are learning remotely.

In these extraordinary circumstances, following your safeguarding policies has never been more important. Your understanding of the child may change due to reduced contact and seeing them in a home setting. Make sure your safeguarding policies are robust enough for this situation.

Your Workspace

- Find a suitable space to work and strike a balance between work and family, and fun
- Set reasonable daily goals
Workload should not increase
- Be clear about how your work-provided device can be used (if you have one)

Staff Communications

- Only use work devices for work, and personal devices for personal (if possible)
- Informal online staff groups should be voluntary and not used for official communications

Data Protection

- For any data protection related questions, speak to your data protection officer (DPO). Data protection exists to protect our personal information and shouldn't be used as a barrier to innovation, especially at the current time. The data protection risks of doing, or not doing something, should be assessed and mitigated in line with legislation.

Working with Students

- Where possible, only use work-provided devices/platforms/systems
- Provide offline activities – not all families have 1-to-1 devices
- Pre-record content for students to access when it suits them
- Only live-stream or use video conferencing with clear permission from school
- Get supervision from another adult, following local guidelines as relevant. If a second adult is not available, record the stream (with necessary policy, permissions and following local guidelines)
- Make sure you and your students follow school policy and understand how to use systems
- Select independent activities for students, there may be limited contact with parents
- Don't forget safeguarding – protect your students from 'bad actors', log/refer any concerns to your safeguarding lead

swgfl.org.uk/coronavirus