King's Hill Primary School

E Safety/Online Safety Policy - 2023

King's Hill is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

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

The school's named online safety leaders: J Hawkins/N. Patel

Our online safety policy has been written by the school, building on advice received and government guidance. It works in conjunction with the school devised acceptable use policy. It has been agreed by senior management and approved by governors.

The school will monitor and enforce the policy through:

- Teacher planning
- Smoothwall Monitor– monitoring of network activity for laptops and desktops (mobile technology not covered- will be put in place when available)
- Log of any incidents – monitored by J. Adams/D. Richards/N. Matharu
- Online safety team at Walsall Education
- Technical Staff to ensure all security software, including virus software and settings are kept up to date

Every member of the school community has a duty of care to online safety as part of safeguarding. This policy deals with incidents associated with the use of technology that affects our school community.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Staff and pupils must read and agree the acceptable use policy before using the equipment in school. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities. Incidents that occur outside of school are covered by parent's duty of care. Those incidents that involve the relationship to school or involve the school may be dealt with by the school.

The Education and Inspections Act 2006 empowers Headteachers 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 online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 online safety behaviour that take place out of school.

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Monitoring Software

Smoothwall Monitor is used across the network in order to

- Monitor inappropriate use of devices including incidents of cyberbullying, offensive use, cybercrime and user vulnerability.
- Monitor internet usage of words associated with the PREVENT agenda
- Enforce the agreement of the Acceptable Use Policy

Online Safety in the curriculum

Online safety will be taught to children across the school from Nursery to Year 6, termly. Online safety training will be included within the Personal Social and Health Education (PSHE) curriculum and children will be reminded at the beginning of any session using ICT equipment.

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 online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/ cross curricular links to other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- Internet use should be 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.
- Where pupils are allowed to freely search the internet, staff should plan the keywords to be used as search terms, checking them for inappropriate content and be vigilant in monitoring the content of the websites the young people visit.

Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way both at home and at school. Kings Hill Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local Online safety

campaigns. Parents and carers will be encouraged to support the school in promoting good Online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events (reminder given at the beginning of assemblies)
- access to parents' sections of the website / pupil records
- their children's personal devices in the school (where this is allowed) and at home

Where an incident occurs within school the child's parents will be given appropriate advice for the use of technology at home.

Visitors to school

Whilst the nature of a visitor's Internet use will clearly vary depending upon the purpose of their visit, it is still important to explain the school's expectations and rules regarding safe and appropriate Internet use to them. These differ slightly to those given to pupils to acknowledge the different situations in which visitors will likely be using the Internet:

- I will respect the facilities and devices on offer by using them safely and appropriately.
- I will not use the Internet for: personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites or content.
- I will report any unpleasant material to a member of staff immediately because this will help protect myself and others.
- I will not download/install program files to prevent data from being corrupted and to minimise the risk of viruses.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details with others.
- I will not carry out personal or unnecessary printing when using the Internet due to the high cost of ink.
- I understand that the school will check my computer files and monitor the Internet sites I visit.

These will be on a paper copy and signed by the visitor

Communication

The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

Pupils may only use approved electronic communication accounts on the school system (e.g. email, blog, text) Children will be told they must immediately save and tell a teacher if they receive an offensive message. Pupils are directed to use school agreed systems for learning for example, Google classroom.

Staff should use a school email communication for anything work related and no other email address or communication systems. The forwarding of chain communications is not permitted.

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

Personal devices
Staff use:

The use of personal devices should not be in the classrooms especially during the school day (8.30 - 3.30) excluding lunchtimes in the staff room or outside when children are not present. They should be locked away in a staff locker for the remainder of the day.

Personal devices are only permitted to be used on school trips away from children in an emergency (you should still have sight of the children), by the lead teacher for the visit.
The concerns relating to mobile phones are based around the issues:

- Staff being distracted from their work with children
- The use of mobile phones around children
- The inappropriate use of mobile phones

Pupil use:

Pupils in Year 6 who have permission to walk home alone will be allowed to bring a mobile phone into school if required. The device will be handed into the office at the start of the day. Pupils will need to collect it at the end of the day.

Communication technologies use in school

Staff/adults:

	Allowed	Allowed at certain times	Allowed by selected staff	NOT allowed
Mobile phones may be brought into school	✓			
Use of mobile phone in lessons				✓
Taking photos on mobile phone/cameras		✓		
Use of other mobile devices		✓		
Use of personal email addresses in school/ school network				✓
Use of school email for personal emails				✓
Use of messaging apps				✓
Use of social media/blogs				✓

Pupils:

	Allowed	Allowed at certain times	Allowed if permission given	NOT allowed
Mobile phones may be brought into school			✓	
Use of mobile phone in lessons				✓
Taking photos on mobile phone/cameras				✓
Use of other mobile devices				✓
Use of personal email addresses in school/ school network				✓
Use of school email for personal emails				✓
Use of messaging apps				✓
Use of social media/blogs				✓

Digital images in the school community

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupil's instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• 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.

• In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases child protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images. Parents will be reminded of this at the beginning of any events where they are able to take images/videos.

• Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the school policy concerning the sharing, distribution and publication of those images which prohibits such activity. Those images should only be taken on school equipment, which should not be taken home; the personal equipment of staff should not be used for such purposes. No mobile phone is allowed in classrooms. Visitors must not use mobile phones in learning environments and storage for their phones will be offered if required.

• Care should be taken when taking digital / video images that pupils are appropriately dressed (e.g. school uniform or PE kit) 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. For example, a child must ask another before taking their photo.

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. For example, no names and image or first name and initial and no image

• Pupils' full names will not be used anywhere on a website, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Social networking and personal publishing

The school will control access to social networking sites, they will be restricted as appropriate through the filtering system. Pupils will be educated in the safe use of such sites alongside the use of relevant child friendly websites.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm **must** be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk for school related social media accounts

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

- The school's use of social media for professional purposes will be checked regularly by the senior leaders to ensure compliance with the school policies.

  There should be –

  - A process for approval by senior leaders

- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Managing filtering

The school will work with LA ICT to ensure systems to protect pupils are reviewed. A filtering system is in place but if staff come across unsuitable on-line materials, the site must be reported to the Online safety team. If pupils come across unsuitable on-line materials, the site must be reported to their teacher who will inform the Online safety team. Staff **are** now able to access sites such as 'You Tube' and others on request but staff need to be aware that these sites do contain inappropriate materials and therefore children are not allowed to use these sites. **Links and content should be checked in school just prior to use in the classroom due to daily rotation of advertising content and changes in filtering.**

Technical security

The school will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.** This means everyone will have a unique login and password
- **All users will be provided with a username and secure password by** LA ICT who will keep an up to date record of users and their usernames. **Users are responsible for the security of their username and password**.
- **From KS1 all users will be taught to login at the beginning of the year. KS2 will be encouraged to generate secure passwords and change these with teachers permissions.**
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept secure
- LA ICT is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly

monitored. The school use Netsweeper to filter the internet for users. LA ICT need to be contacted for changes to this filtering process by the headteacher.

- **Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet but they are not 100% safe so staff should be vigilant whilst pupils are using devices.**
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils etc)
- Walsall council Online monitoring service regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- School devices are not for personal use that users (staff/students/pupils/community users) and their family members are **not** allowed on school devices that may be used out of school.
- Staff are forbidden from downloading executable files and installing programmes on school devices.
- The school does allow the use of removable media (encrypted memory sticks only) by users on school devices. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**. (See school data protection policy for further information)

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. online bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	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				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files						X

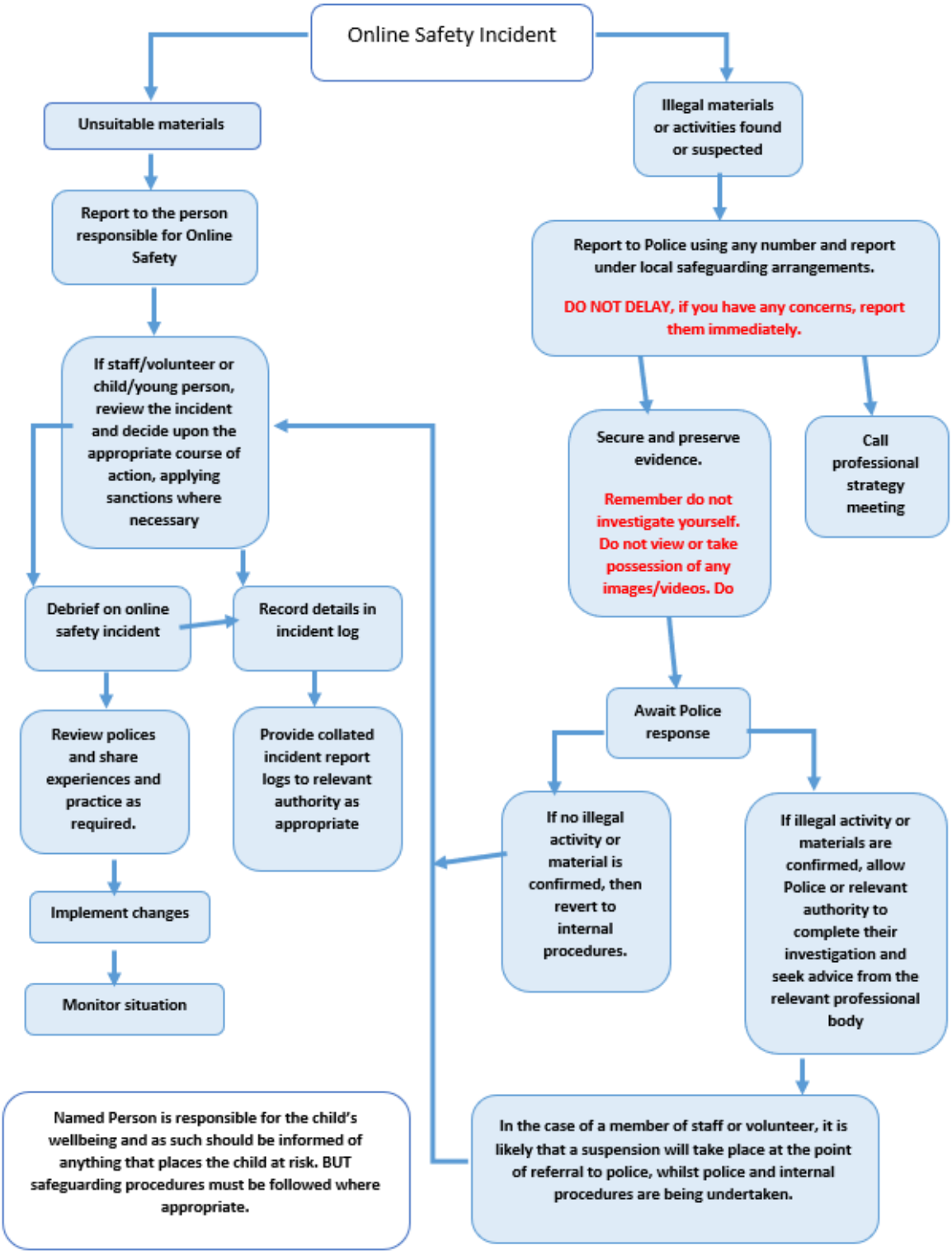
• Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. School will deal with matters internally but seek advice from the police if required. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways.					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)			X		
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce			X		
File sharing			X		
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need 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 involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff 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
    - 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
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

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 of misuse of devices and school systems are dealt with as soon as possible in a proportionate manner and in accordance with the school policy (refer to code of conduct and behaviour policies). Each incident listed below will be referred to the appropriate personnel and sanctions will follow as necessary.

School will ensure that members of the school community are aware that incidents have been dealt with.

Pupils Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanctions e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal		X	X					X
Unauthorised use of non-educational sites during lessons	X	X		X	X		X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X			X		X	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X		X	X		X	X
Unauthorised downloading or uploading of files	X	X		X	X		X	X
Allowing others to access school/network by sharing username and passwords	X	X			X		X	X
Attempting to access or accessing the school/network, using another pupil's account	X	X		X	X		X	X

Attempting to access or accessing the school/network, using the account of a member of staff	X	X		X	X		X	X
Corrupting or destroying the data of other users	X	X		X	X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X	X		X	X
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X		X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X			
Using proxy sites or other means to subvert the school's filtering system	X	X		X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X		X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X		X	X		X	X

Staff Incidents	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).	X	X			X	X
Inappropriate personal use of the internet/social media/personal email	X		X	X	X	X

Unauthorised downloading or uploading of files	X		X	X	X	X
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	X		X	X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X		X	X	X	X
Deliberate actions to breach data protection or network security rules	X		X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X	X	X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils	X		X	X	X	X
Actions which could compromise the staff member's professional standing	X		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X		X	X
Using proxy sites or other means to subvert the school's filtering system	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X
Breaching copyright or licensing regulations	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X		X	X	X	X

Review: July 2023

Next review – July 2024

King's Hill Primary School

Acceptable Use Policy Statement - 2023

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users including pupils should have an entitlement to safe access to the internet and digital technologies at all times.

The school will try to ensure that staff/volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

The school will try to ensure pupils will have good access to digital technology to enhance their learning opportunities and will, in return agree to be responsible users.

Staff/volunteers

Acceptable Use Agreement for staff/volunteers is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems, school data and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

Pupils

Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect our pupils to agree to be responsible users.

King's Hill Primary School

Acceptable Use Agreement – September 2023

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school / academy* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 a lawful basis or their express permission and informed consent.
- 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 / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg 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 social networking sites in school in accordance with the school's policies.
- I will only communicate with students / 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 / academy*:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. 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.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (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 / academy policies.
- 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
- I will not disable or cause any damage to school equipment, or 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 (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be

encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student / 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 / academy or policy to disclose such information to an appropriate authority in line with our legal or contractual obligations.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school 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 the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school / academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include 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 digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

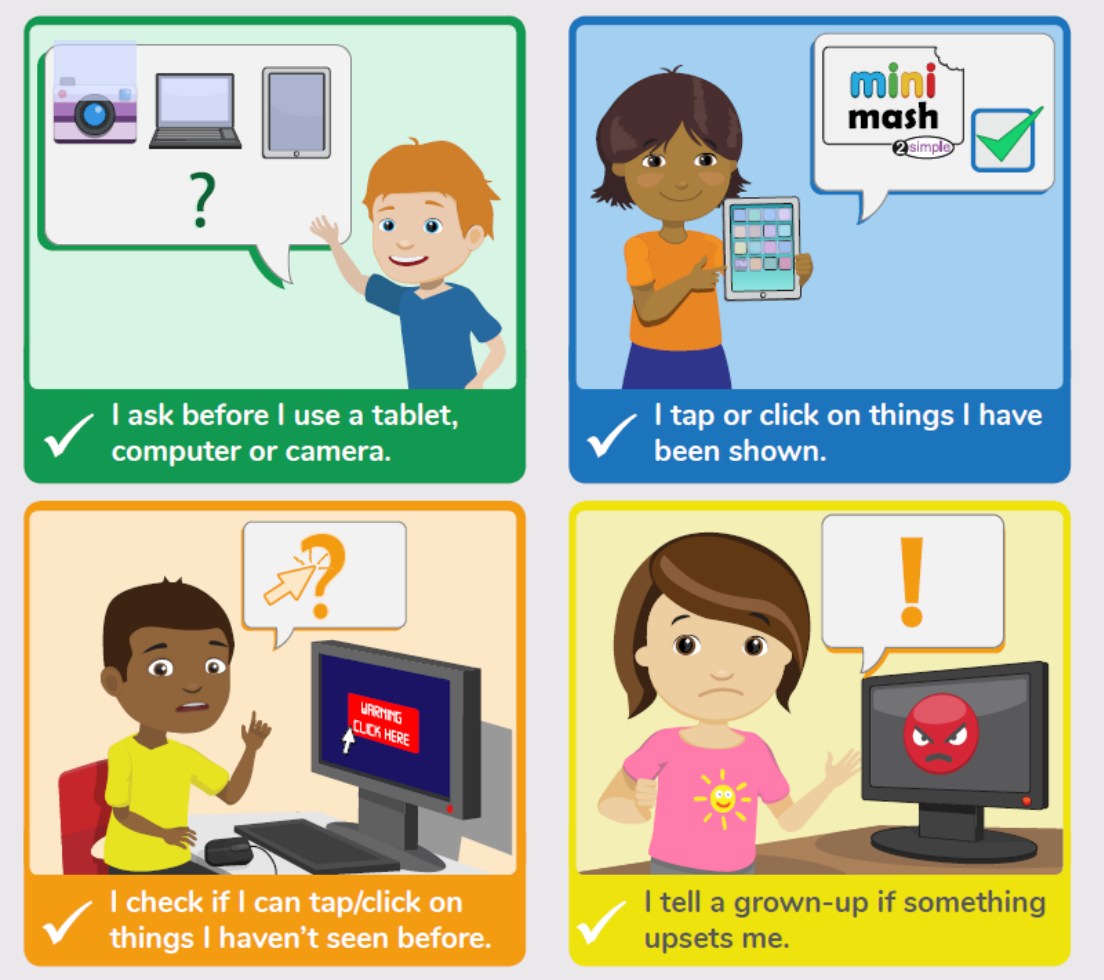
Date: .....

Updated July 2023

King's Hill Primary School

Pupil Acceptable Use Agreement – September 2022

EYFS



Key Stage 1

I will ask a teacher or suitable adult if I want to use the computer.

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable 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

Key Stage 2

I understand that the school will monitor my use of the computer/iPad.

I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.

I will be aware of 'stranger danger' when I am communicating online.

I will not tell anyone my personal information about myself or others online.

I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language. I appreciate that others may have different opinions.

I will not take or distribute images of anyone without their permission.

I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices.
- I use my own equipment out of the school in a way that is related to me being a member of this school

Name of Pupil: ……

Class: ……..

Signed: ……..

Date: ……..

Parent / Carer Countersignature ……

NM – July 2023