St John's C of E Primary School

ST JOHN'S CE
PRIMARY SCHOOL

Policy
For
Online Safety

Policy written by: AM
To be reviewed September 2024

Reviewed: Sep 2023

Online Safety Policy

Online Safety encompasses Internet technologies and electronic communications such as mobile devices as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. All members of the school community have a responsibility to ensure technology and in particular the internet is used in a safe way.

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Walsall Network including the effective management of Smoothwall Monitor monitoring *and/or other filtering service (Netsweeper)*
- National Education Network standards and specifications.

School online safety policy

- The online safety Policy is part of the School Development Plan and relates to other policies including those for Computing, bullying and for child protection and safeguarding.
- Our online safety Policy has been developed by senior management, digital leaders and School Council prior to being approved by governors and the PTA.
- The online safety Policy and its implementation will be reviewed annually.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the Online safety Policy. In accordance with KCSiE September 2023 Governors should ensure they have had training on an annual basis about online safety.

School responsibility

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. 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. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Keeping Children safe in Education September 2023 states 'As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material…support governing bodies and proprietors keep their children safe online (including when they are online at home)'

Incidents

The breadth of issues classified within online safety is considerable, but can be categorised in to four areas of risk:

• content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• contact: being subjected to harmful online interaction with other users; for example: 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; for example, 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 scams

Reporting incidents

- Any incidents are to be logged on CPOMs

Teaching and learning

Why Internet use is important

- The Internet is an essential element for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

Online Safety is part of our curriculum. Our school curriculum includes digital literacy which is taught as part of computing units from Purple Mash as well being supported by Project Evolve. Project Evolve is related to the objectives in Education for a connected world and also allows staff to understand the teaching that needs to be in place. This is based on the assessment of the pupil's current understanding through the use of knowledge maps in Project Evolve. This is also enhanced with regular sessions related to online relationships in our PHSE/RSE curriculum, assemblies and national events including safer internet day, anti-bullying week.

The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing Internet Access

- Walsall Council School ICT service will monitor and review regularly the information system security, School ICT systems capacity and security.
- Security strategies will be discussed with ICT- School Services as and when appropriate.

Monitoring

The school will monitor and enforce the policy through: e.g.

- Smoothwall monitor Monitoring- provides the most advance monitoring that is moderated by vast AI technology and human specialists. Schools are alerted immediately should an incident arise. Smoothwall monitor is the only solution of its kind that continuously builds a profile of all users, allowing the system to accurately interpret between a one-off event as well as a consistent pattern of behaviour.
- Teacher planning
- Log of any incidents: Will be dealt with by A Mills, K Oakley and S Wynne.
- Online safety survey for children –
- Online safety team at Walsall Education
- Technical Staff as part of SLA agreement with Walsall Council ICT services 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. 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.

Monitoring solution

Smoothwall Monitor is used across the network in order to

- Monitor inappropriate use of language
- Monitor internet usage Inc. words associated with the prevent agenda
- Enforce the agreement of the Acceptable Use Policy (See Appendix)

Any identified incident is reported to A Mills, K Oakley and S Wynne in order for it to be investigated and dealt with. Incidents of every level are also monitored and reported by the Local authority online safety advisor and reported via email.

A weekly report that is a reassurance email that gives an update on the number of users (people who log into devices), the number of devices that are being monitored and number of captures in the week. A monthly report is sent that includes details relating to school captures and incidents. This helps and supports us to identify the risk profile and look at patterns in the captures.

The monitoring software does not negate the need for staff to supervise pupils when using devices and it should be noted that it works on networked devices and chromebooks but not iPads. iPad use should be fully supervised by staff and websites given to pupils in order to reduce the risk of coming across inappropriate content.

Managing filtering

- The school will work with ICT-School Services and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the head teacher.
- SMT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor ICT-School Services can accept liability for the material accessed, or any consequences of Internet access.
- Where the use of the internet is pre planned, staff will check websites before sharing links with pupils in order to ensure that sites are suitable for pupils. When using videos staff must check the content before using the video. Videos should be downloaded or embedded in a presentation in order to make sure no adverts or additional videos are played prior or after the desired content.
- Karen Oakley, Online safety lead, will ensure that the school's filtering system is working by randomly checking logins and devices, half termly, using 'test filtering' www.testfiltering.com. A screen shot of the checks will be made and saved on the school's network.

Safe use of the Internet in teaching and learning

- Pupils' access to the Internet will be under adult supervision at all times.
- All use of the schools Internet access is monitored, including that by staff, parents and any other members of the community. Pupils are informed that Internet use is monitored.
- The school works in partnership with pupils, parents and the LA to ensure systems to protect pupils are reviewed and improved as appropriately.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the DSL and then the LA to be blocked.
- Senior staff ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Virus protection is installed and updated regularly.
- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR).
- Files held on the school's network are regularly checked. The school ICT systems are reviewed regularly with regard to security.

Communication

- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the website particularly in association with photographs except where parental permission has been given for exceptional circumstances for e.g. 'Values Award' winners.
- Parents will be given the opportunity to opt out of allowing their child's work or photograph to be published on the school website or other media such as Twitter and Class Dojo.
- Pupil's work can only be published with the permission of the pupil.

Social networking and personal publishing

- Staff should refer to the school's social media policy
- The school will block/filter access to social networking sites for pupils, staff have access to appropriate social media e.g. Twitter.
- Staff should not be 'friends' online with any St John's pupils.
- Staff should not publish any photographs or comments about school on any website without the permission of the Head Teacher

When official school social media accounts are used there is:

- A process for training in the effective use of Twitter
- Passwords for each phase account are held by the office manager as well as the teaching staff in that phase
- The code of behaviour for users of the accounts, includes systems for reporting and dealing with abuse and misuse as well as understanding of how incidents may be dealt with under school disciplinary procedures

Mobile Technology

- The use of staff and visitor mobile devices should not be in the classrooms especially during the school day (8.00 - 3.30 school time and also after school clubs) excluding lunchtimes in the staff room, and only the school phone used on school trips away from children in an emergency.
- All devices should be silenced and prevented from receiving notifications during school hours.
- Pupils who bring in mobile devices should turn off the devices when entering school, hand them into the school office for safe keeping until being return to the child at the end of the school day.
- Teacher's iPads are required to have a secure password on them before leaving school site to protect data.

Use of digital and video images – See also GDPR policy

- When using digital images, staff should inform and educate students / 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.

- Written permission from parents or carers is obtained before photographs of students are published on the school website / social media / local press

Password security

- Staff are responsible for managing their own passwords for the network and websites used as part of school life but should be mindful of what they are using as passwords. Three random words with a mixture, numbers and punctuation is the recommended password format. All passwords should be different for every site or programme. Staff are encouraged to use password managers.

- Pupil passwords should be kept secure. For EYFS these should be easy to type and unique for each pupil. KS1 and KS2 pupils use a generated username and a generated password for them. Passwords are appropriate for each user age group.

- Network passwords and associated apps or sites are managed by the school technical support team.

School network security

- The school is supported by Walsall Schools technical support who maintain and support the school with antivirus and technical network security. All incidents of this nature should be reported to them in the first instance.

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. We will take every opportunity to help parents understand these issues through parents' evenings, 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
- access to parents' sections of the website / pupil records
- their children's personal devices in the school (where this is allowed)

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

If using the internet at home:

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Students should only invite known friends and deny access to others.

Remote education

Remote education is included in our safeguarding considerations please consult our remote learning policy for more information.

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 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.

- 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 for websites 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 may check my computer files and monitor the Internet sites I visit.

Dealing with pupil and staff incidents

	Actions / Sanctions							
Pupils Incidents	Refer to class teacher / tutor	Refer to Head teacher /SLT	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 sanction e.g. exclusion
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	x	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	
Unauthorised / inappropriate use of social media / messaging apps / personal email	x	x	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	x	x		x			x	
Attempting to access or accessing the school network, using another pupil's account	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	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x	x	x	x	
Continued infringements of the above, following previous warnings or sanctions	x	x	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	x	x	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	x	
Deliberately accessing or trying to access offensive or pornographic material	x	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 and the Online safety policy

All staff will receive in house online safety update training on an annual basis. Staff are informed that network and internet traffic will be monitored and can be traced to the individual user. Staff will always use a child friendly safe search engine when accessing the web with pupils, for example www.swiggle.org.uk

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

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:

	Actions / Sanctions							
Staff Incidents	Refer to line manager	Refer to Head teacher /SLT	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	x	x	x	x
Inappropriate personal use of the internet / social media / personal email	x	x	x	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		
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	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	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x		x	x	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students.	x	x	x	x	x	x	x	x

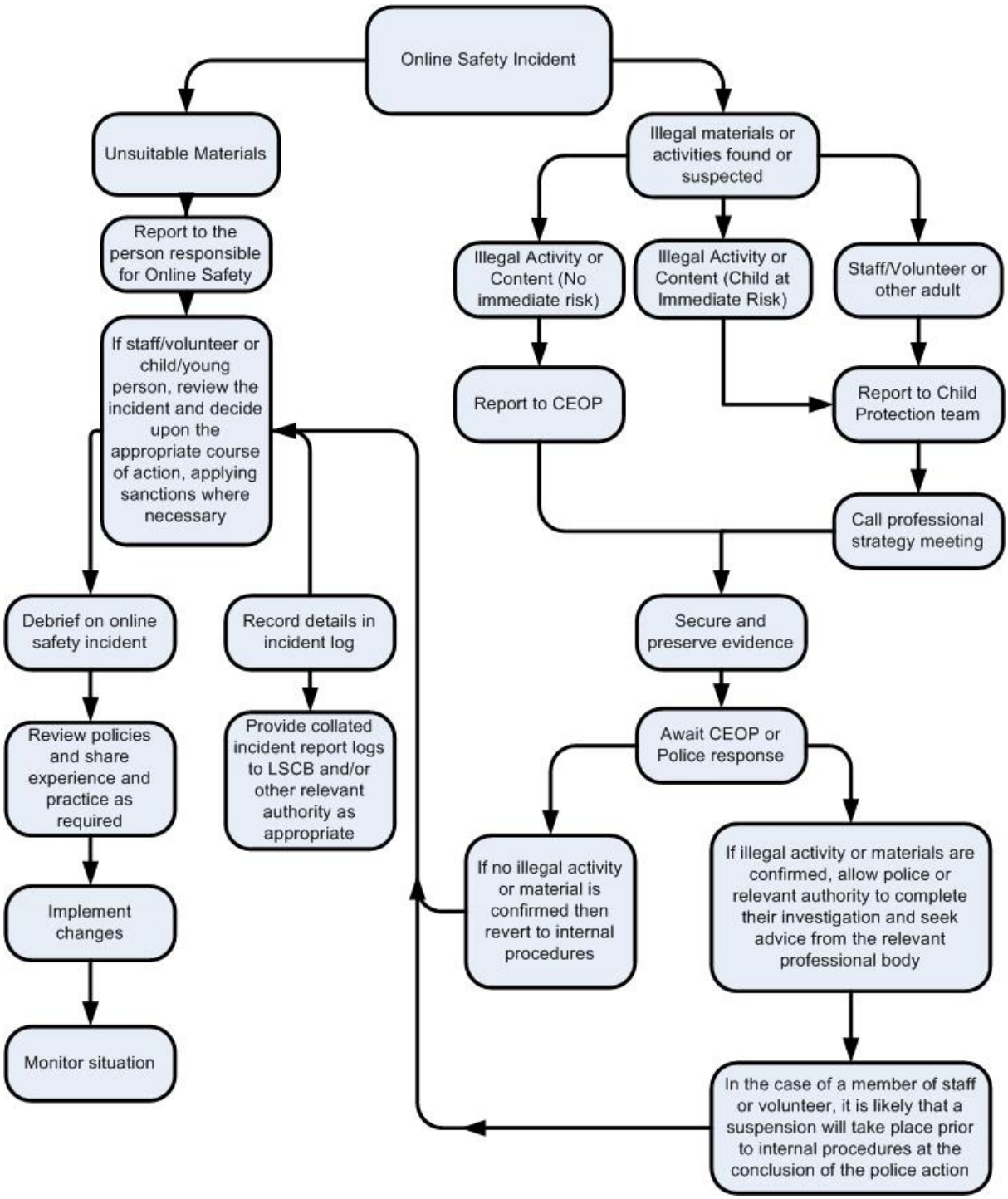
Actions which could compromise the staff member's professional standing	x	x	x			x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	x	x	x			x	x	x
Using proxy sites or other means to subvert the school's filtering system	x	x	x	x	x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			x	x		
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x
Breaching copyright or licensing regulations	x	x				x		
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x		x	x	x

Responding to incidents of misuse

This guidance is intended for use when staff members 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

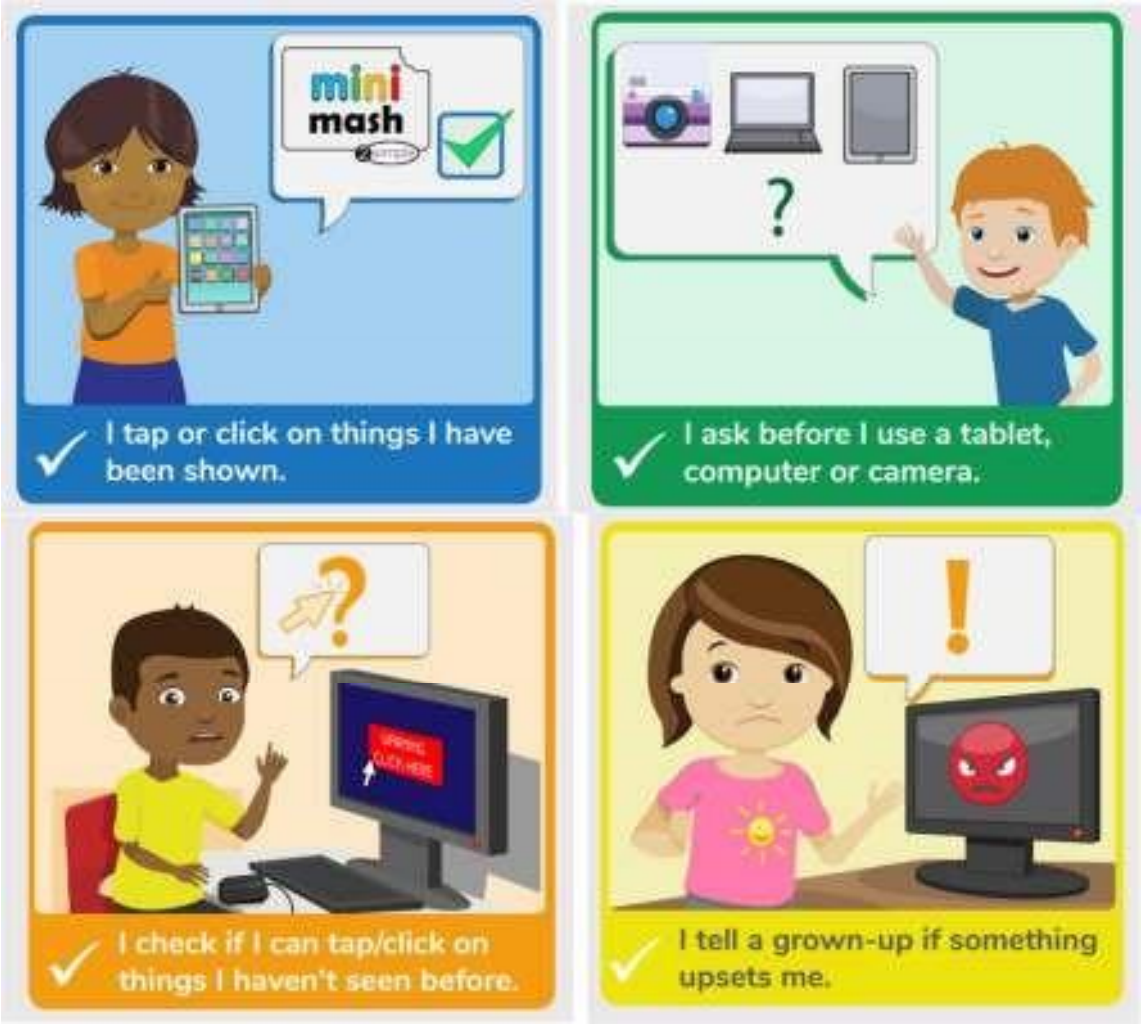
Illegal Incidents

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.



Pupil Acceptable Use Policy Agreement

Early Years



My name: .....

Date: .....

Pupil Acceptable Use Policy Agreement

Key Stage 1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- 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 / tablet

Signed(child):……

Date:……

Pupil Acceptable Use Policy Agreement

KS2

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.
  T= Is it true?
  H= Is it Helpful?
  I = Is it Inspiring?
  N = Is it Necessary?
  K = Is it Kind?
- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

My name: ……

Date: ……

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

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 should have an entitlement to safe access to the internet and digital technologies at all times. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Keeping Children safe in states 'As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material…support governing bodies and proprietors keep their children safe online (including when they are online at home)'

This Acceptable Use Policy 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 systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and 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.

Acceptable Use Policy Agreement

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 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, 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 not use the systems for personal or recreational use within the policies and rules set down by the school due to the cybersecurity risks.

- 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 set strong passwords (a strong password is one which uses a combination of letters, numbers and other permitted signs)

- 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 Computing 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 / 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 (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- 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:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices, smart watches 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 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 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, 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 Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted.
- 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 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.

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 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
- 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: .....