



Our Vision

All things are possible with God. Matthew 19-26

At Little Bloxwich Church of England Primary School we see that everyone is unique and they are valued for this. Together we flourish socially, spiritually, emotionally and academically. We are part of God's family and everyone is expected to treat each other with kindness and respect as Jesus taught us to.

Little Bloxwich Primary School

Online Safety Policy

Policy Adopted: September 2023

Review Date: September 2024

Little Bloxwich Primary School prides itself on providing a safe, stimulating and engaging learning environment. All relationships within the school are built on the highest levels of respect.

At Little Bloxwich, all pupils are supported, nurtured and challenged in order that they meet their full potential.

Pupils, staff and parents feel safe within the school and know that the leaders of the school will help in any way possible.

The purpose of the online safety policy.

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to online safety. The policy relates to other policies including Computing curriculum, Staff Code of Conduct, Anti-Bullying, Behaviour, Safeguarding Children and Health and Safety.

Writing and reviewing the online safety policy.

Miss Oliver, Deputy Head Teacher and Deputy Designated Safeguarding Lead is the Online Safety Coordinator who will work closely with Mrs Taylor, Head Teacher and Designated Safeguarding Lead.

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 a pink form and handed directly to DSL (Mrs Taylor) or DDSL (Mrs Robinson/Miss Oliver) in Mrs Taylor’s absence. The incident will then be dealt with accordingly. The incident and the actions taken will be logged onto SIMS by the DSL/DDSL.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life 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

- The school Internet access will be designed expressly for pupil use and will include 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.

Online Safety in the curriculum

A programme of training in online safety will be taught to children across the school from Reception to Year 6. We use Purple Mash as a tool to teach online safety, which is taught discretely at the start of each term and we take part in the national events. This links to Education for a connected world objectives in an age appropriate lesson. As well as this online safety is continually reinforced during the weekly computing lessons.

In addition to this as part of the computing curriculum the following is taught:

Early Years Foundation Stage and Key Stage 1

At this level, use of the Internet will either be quite heavily supervised or based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult. Children will be taught key skills of logging on, how to complete safe searches and what is appropriate and inappropriate.

Lower Key Stage 2

Children will now be given more opportunities to develop their digital literacy skills (e.g. sending polite and friendly messages online to other children, the need to create strong passwords etc.). They will be shown how to develop a responsible attitude towards searching the Internet and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Upper Key Stage 2

Children will now be encouraged to become more independent, agreeing to the acceptable use policy first, before searching for information on the Internet using a child friendly search engine, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

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: Mrs Taylor, Miss Oliver and Mrs Robinson (PSA)
- Online safety survey for children –
- Online safety team at Walsall Education
- Technical Staff as part of SLA agreement with LA ICT 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 Mrs E Taylor (Miss Oliver - Online Safety lead or Mrs Robinson - PSA in Mrs Taylor's absence) 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 LA ICT to ensure systems to protect pupils are reviewed. If staff comes across unsuitable on-line materials, the site must be reported immediately to the online safety Coordinator. If pupils come across unsuitable on-line materials, the site must be reported to their teacher who will inform the online safety Coordinator. 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 ability to access in school.**

Miss Oliver (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.

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.

Communication

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.

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

Mobile devices

The use of staff and visitor mobile devices should not be in the classrooms especially during the school day (8.45 - 3.30) excluding lunchtimes in the staff room, and only 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.

Digital images in the school community - See also Data protection policy for school

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 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; 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 (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.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Written consent 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.

Social networking and personal publishing

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

Pupils, staff and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Pupils will be advised and taught through the curriculum to use nicknames and avatars when using social networking sites. Staff must not make 'friends' or communicate with current pupils or pupils that have left on any social network site, i.e. Facebook, Instagram. Staff should check that their privacy setting is set to the most secure setting and also consider changing their profile name and picture. Staff who choose to use 'Facebook' and other network sites do so at their own risk and should be aware of the School's Code of Conduct.

Pupils will be taught when 'gaming' i.e on Playstation, Xbox, Nintendo or PC, they should only communicate with people they know rather than unknown gamers and play age appropriate games.

Managing 21st century technologies

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

School staff should be aware that mobile technologies with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Personal devices, including mobile phones, will not be used during lessons or formal school time unless express permission is given by the Head or Deputy Head. Personal devices must not be accessed (e.g. in another room or locked away) when children are present. The sending of abusive or inappropriate messages or files by Bluetooth or any other means is forbidden. Staff will be issued with a school phone where contact with pupils or a parent is required. **Staff will not use personal devices to capture images/videos of pupils.**

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2019. Refer to the School's data handling policy. Staff must encrypt memory sticks to store any personal data relating to work that needs to leave the school premises. This should be the only form of data storage that staff uses. **Staff should ensure that the device is not left unattended.**

Staff should not walk away from any device without first locking it.

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 year of entry - surname - initial and a generated password for them.

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

School network security

The school is supported by LA ICT 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.

Authorising Internet access

Parents will be asked to sign and return a consent form.

Handling Online safety complaints

Complaints of internet misuse will be dealt with by an online safety coordinator or the Head. They need to be recorded on an online safety incident form. (See appendix three) Any complaint about staff misuse must be referred to the head teacher or LADO (01922 654040)

Complaints of a safeguarding nature must be dealt with in accordance with school's safeguarding procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet.

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

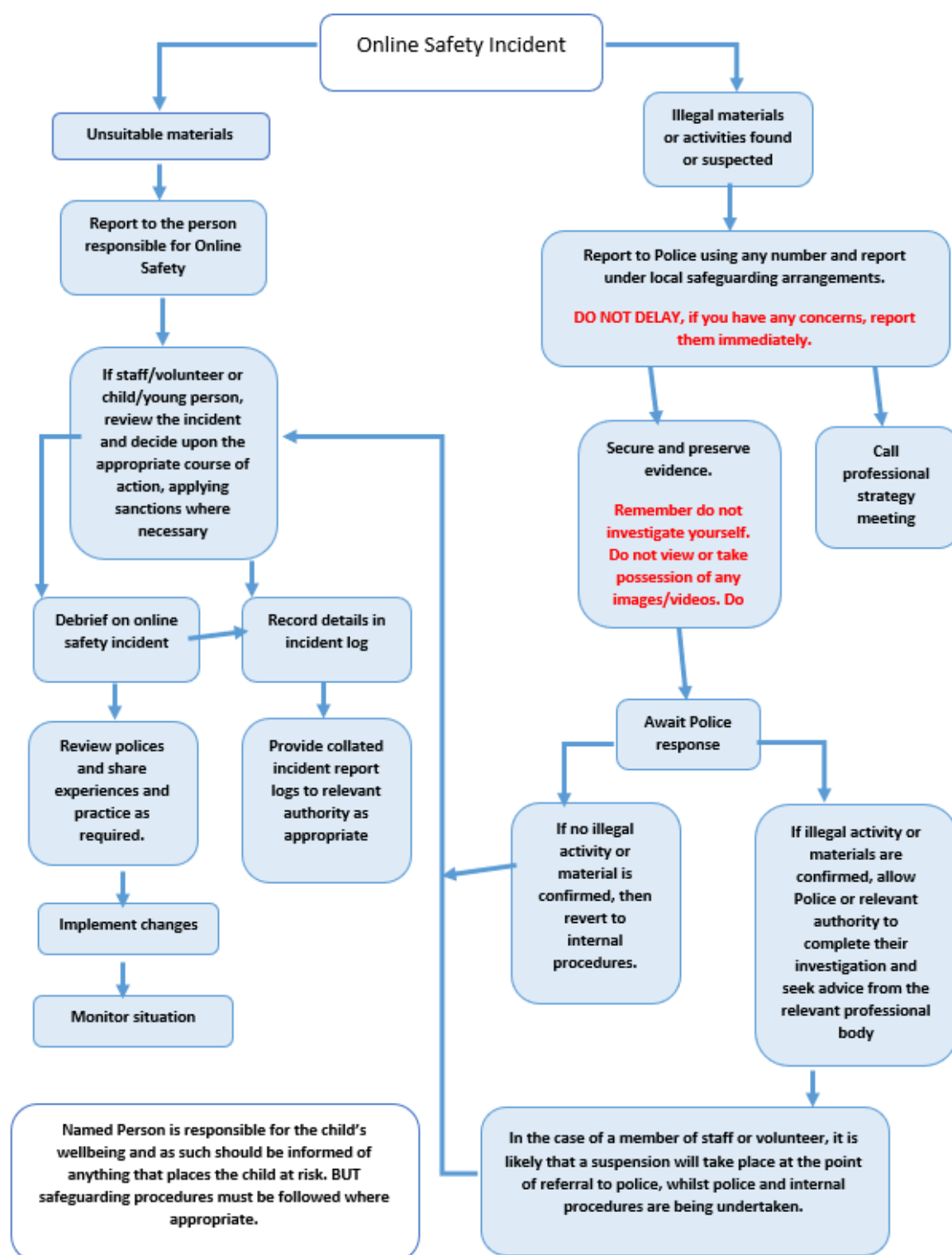
Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

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:

Pupil Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / 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
Unauthorised use of non-educational sites during lessons	X				X		X	
Unauthorised use of mobile phone / digital camera / other handheld device	X	X			X		X	
Unauthorised use of social networking / instant messaging / personal email	X	X			X		X	
Unauthorised downloading or uploading of files		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 student's / 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		
Corrupting or destroying the data of other users		X			X	X		
Sending an email, text or instant 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
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	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/Sanctions:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for	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
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		X			X	X		
Unauthorised downloading or uploading of files		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							
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		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 instant message that is regarded as offensive, harassment or of a bullying nature		X	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		
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		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions								X

Incidents



To be reviewed September 2024

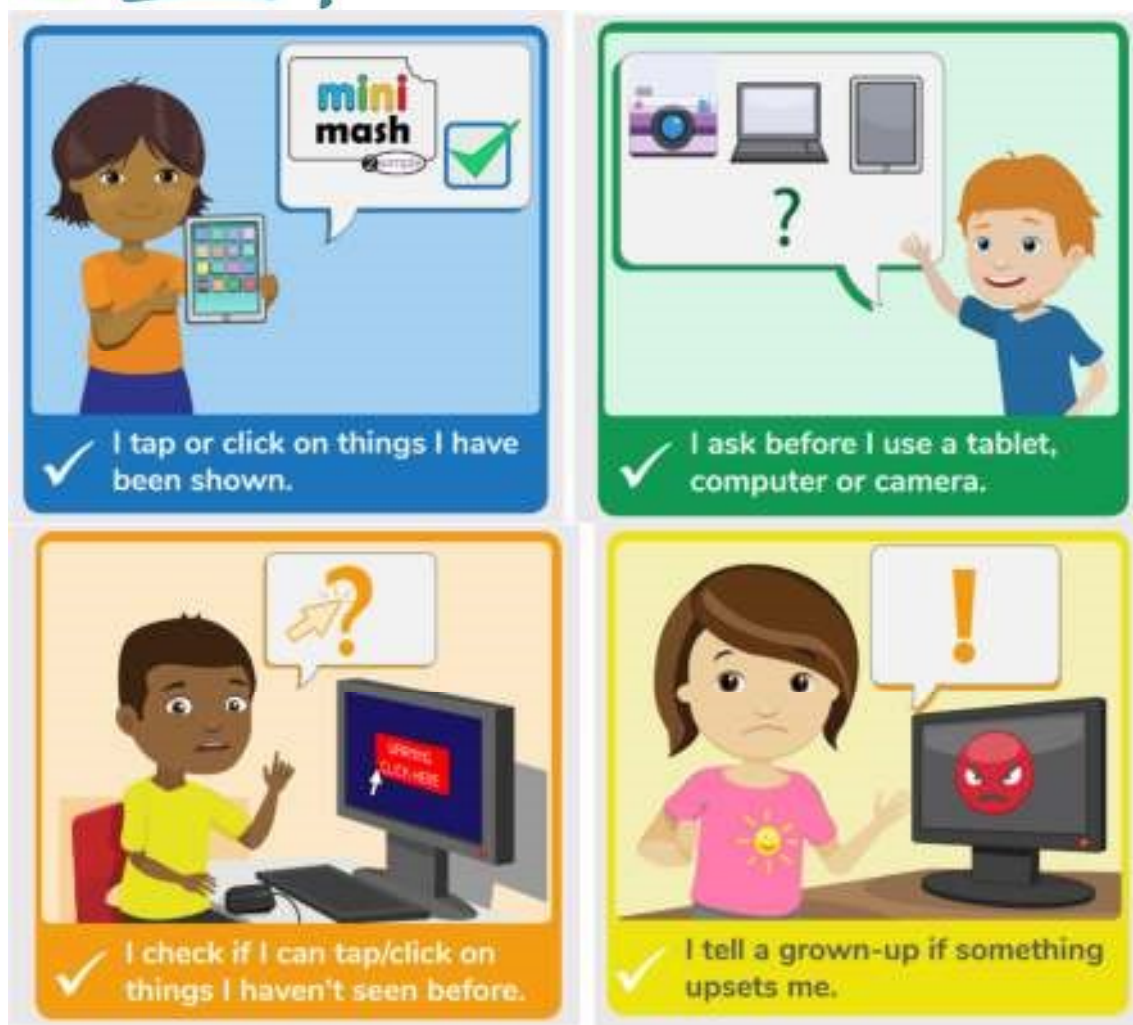
AUP:

Purple Mash

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: