STATHAM COMMUNITY PRIMARY

LYMM

Inspiring all to learn, care and share

E-SAFETY POLICY

Date of Publication : 7th March 2017
Date Ratified : 20th March 2019
Date of Review : January 2020, May 2021

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 is now regarded as an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers at Statham use technology as an integral part of curriculum planning and delivery. Schools are ideally placed to help young people learn to become e-safe. This policy is designed to ensure safe internet use by pupils in school and also while online beyond the classroom environment.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

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

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety policy is used in conjunction with these school policies

- Behaviour/Anti-bullying
- Child Protection
- Loaning School Equipment
- Remote Learning
- Teaching and Learning

Roles and Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The role of the governors will include:

- regular liaisons with the designated E-Safety Co-ordinator
- attend, where possible any staff E-Safety training
- regular monitoring of E-Safety incident logs

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the community.

The Headteacher/Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles.

The Headteacher/Senior Leaders/E-Safety Coordinator will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher and Deputy should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff (Appendix 1 - ICT Misuse / E-Safety breach Reporting Protocol).

E Safety Coordinator

Takes day-to-day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policy/documents.
Coordinates and organises a team of children responsible for delivering E-Safety advice to classes (E-Safety cadets/digital leaders)
Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
Regular monitoring of E-Safety incident logs
Organises training and advice for staff
Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
Liaise with technical support staff

The ICT Technician is responsible for ensuring:

The school's ICT infrastructure is secure and is not open to misuse or malicious attack
The school meets the E-Safety technical requirements as advised by Becta and the Acceptable Use Policy
The school's filtering policy (Warrington Borough Council), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
That he/she keeps up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
That the use of the network/Learning Platform (through our website)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator for investigation/action/sanction
That monitoring software/systems are implemented and updated

Teaching and Support staff are responsible for ensuring that:

They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
They have read, understood and signed the school Staff Acceptable Use Policy/Agreement (Appendix 2)
They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation/action/sanction and fill in an E-Safety concerns form
E-Safety issues are explicit and embedded in all aspects of the curriculum and other school activities (Long Term Planning/Yearly Overview) including Statham's Rights and Responsibilities.
Pupils understand and follow the school E-Safety and acceptable use policy (Appendix 3 – Pupil e-Safety Agreement)
Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
They monitor ICT activity in lessons, extra-curricular and extended school activities including daily spot checks of browser history.
iPads are not used during wet break times and all devices are locked into apple classroom.
iPads and laptops are returned and plugged in at the end of each school day-class monitors
They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
In lessons where internet use is pre-planned 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.
They only use You Tube on the interactive whiteboards as a teaching and learning tool. Children should not use You Tube at any time and may use Kids Tube under the direction of the class teacher.

Processes are in place to deal with any ICT misuse, these should be implemented if necessary.

Pupils:

Are responsible for using the school ICT systems in accordance with the Pupil E-Safety Agreement (Appendix 3), which they will be expected to sign on a yearly basis, before being given access to school systems.
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
Are expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
In accordance with the E-Safety agreement, children should not access any websites that are only to be used by teachers e.g. You Tube. Children will be aware of the sanctions in place if such an event arises.

Parents/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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters and website information.

Parents and carers will be responsible for:

Accessing the school website to keep up to date with E-Safety news.
Signing the parent/carers Internet usage agreement (Appendix 4)

Contacting school to report any E-Safety issues that concern them
Attending any E-Safety workshops delivered by school

Teaching and learning

E-Safety is a focus in all areas of the curriculum and staff will reinforce E-Safety messages in the use of ICT across the curriculum.
E-Safety is taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.
E-Safety skills will be embedded through both discrete ICT and cross-curricular application.
In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education and training

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy.

Safeguarding/ E-Safety concerns will be discussed at weekly briefing sessions.
This E-Safety policy and its updates will be presented to staff in staff meetings.
The E-Safety Coordinator will provide advice/guidance/training to individuals as required.
Pupils should be taught in all lessons to be critically aware of the materials/content they access online 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.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 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.

Staff may take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes. However, should circumstances require, images may be taken on staff owned equipment provided that at the first available opportunity they are transferred to the school's network / blog and deleted from the staff device.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
Pupils must not take, use, share, publish or distribute images of others without their permission
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.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will not be named and in other places, no full names will be used on the school website/DB learning platform.

Communications

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons		x						x
Use of mobile phones in social time	x							x
Taking photos on personal mobile phones or other camera devices	x							x
Use of hand held devices e.g iPads	x					x		
Use of personal email addresses in school, or on school network	x							x
Use of school email for personal emails				x				x
Use of chat rooms / facilities		x						X
Use of instant messaging				x				x
Use of social networking sites				x				x
Use of blogs		x				x		

When using communication technologies the school considers the following as good practice:

The official school email service may be regarded as safe and secure. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g by remote access). Although there are times when staff are working at home and will send and receive emails to and from the school system. Staff will not send any confidential material in an email unless it is password protected and on the school system.
Users need to be aware that email communications may be monitored
Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
Any digital communication between staff and students / pupils or parents / carers (email, chat,etc) must be professional in tone and content. *These communications may only take place on official (monitored) school systems, e.g. DB Primary/Showbie. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.*
Where possible, whole class or group email addresses will be used by all classes.
Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

Data Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.

- Only transferred to others with adequate protection.

Staff and volunteers must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer personal data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - o the data should be encrypted and password protected
    - o the device should be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
    - o the device should offer approved virus and malware checking software
    - o the data should be securely deleted from the device, once it has been transferred or its use is complete

Sanctions

Staff should follow the reporting protocol when dealing with concerns that they feel are either illegal (involving sexual abuse images, adult material, criminally racist material or criminal activity) or inappropriate (involving cyber bullying, use of restricted websites, revealing personal information or incorrect use of electronic devices, etc.). It is important that any incidents are dealt with as soon as possible in a proportionate manner.

Appendices

- Appendix 1 - ICT Misuse/ E-Safety Breach Reporting Protocol
- Appendix 2-School staff acceptable usage policy
- Appendix 3-Pupil acceptable usage agreement
- Appendix 4-Parent/carers agreement
- Appendix 5- E-Safety Concern Form

Users Actions

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 of school when using school equipment or systems. The school policy restricts usage as follows:

		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					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	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the group or brings the group into disrepute				X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards that are in place					x	
Infringing copyright					X	

Revealing or publicising confidential information (eg financial / personal information, computer / network access codes and passwords)				×	
Creating or propagating computer viruses or other harmful files				×	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				×	
Using the group systems to run a private business				X	
On-line gaming (educational)		X			
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing (eg Bit Torrent, Limewire)				X	
Use of personal social networking sites(while "at work")				x	
Use of an official group social networking site				x	
Use of video broadcasting eg Youtube				x	

Pupil Incidents:	Refer to class teacher	Refer to Police	Refer to Head teacher/ E Safety Lead	Requires technical response / support	Inform parents / carers in line with our behaviour policy	Removal of access to technology / devices	Warning	Further Sanction, e.g. exclusion
Accessing unauthorised non-educational sites during lessons	✕				✕			
Unauthorised downloading or uploading	✕				✕			
Allowing others to access technology / devices by sharing username and passwords	✕				✕			
Attempting to access or accessing the technology / devices, using another person's account (hacking)			✕		✕			
Corrupting or destroying the data of other users			✕		✕			
Sending a communication that is regarded as offensive, harassment or of a bullying nature			✕		✕			
Actions which could bring the organisation into disrepute.			✕		✕			
Deliberately accessing materials that the school has agreed is inappropriate			✕		✕			
Activities that infringe copyright or data protection.			✕		✕			
Using proxy by-pass sites or other means to subvert the filtering system			✕		✕			
Accidentally accessing materials that the school has agreed is inappropriate and failing to report it.			✕		✕			

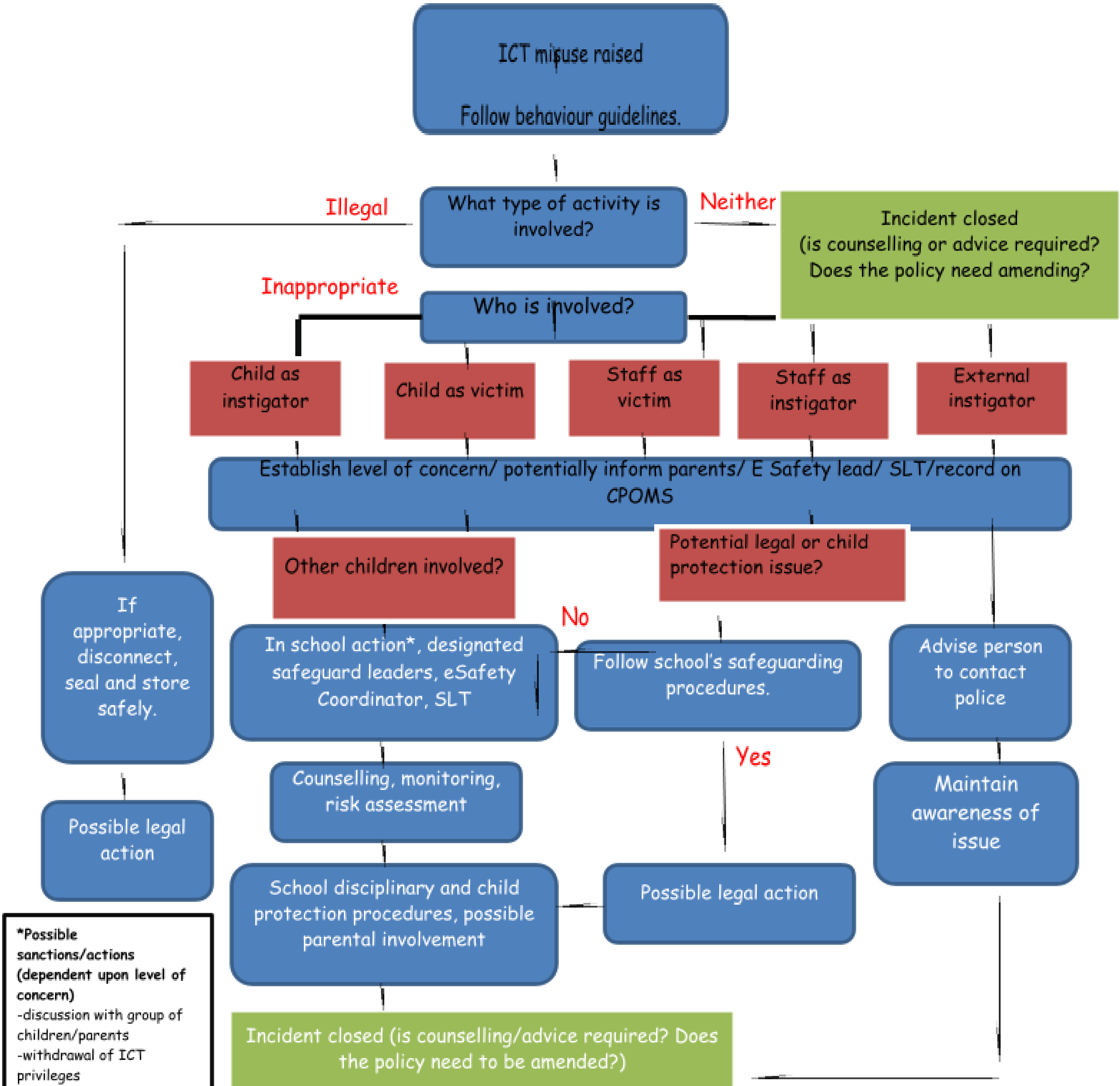
Unauthorised use of mobile phone / digital camera / other handheld device			×		×			
Unauthorised use of social networking / instant messaging / personal email			×		×			

Staff Incidents:	Refer to Head teacher	Refer to LA	Refer to Police	Requires technical response / support	Warning	Suspension	Disciplinary action
Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities).	×	×	×				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email "while at work"	X						
Unauthorised downloading or uploading of files	X						
Disclosing passwords or any information relating to the security of technology and devices.	X						
Accidental infringement of the organisation's personal data policy	X						
Deliberate infringement of the organisation's personal data policy	X	×	×				
Corrupting or destroying the data of other users	×	×	×				
Deliberate damage to hardware or software	×	×	×				
Sending a communication that is offensive, harassment or of a bullying nature	×	×	×				
Using personal communication technologies eg email / social networking / instant messaging / text messaging to communicate with young people (except where allowed in the policy)	×	×					
Actions which could compromise the professional integrity of staff / volunteers	×	×					
Bringing the organisation into disrepute	×	×					
Deliberately accessing materials that the school has agreed is inappropriate	×	×					

Breaching copyright or licensing regulations	X	X					
Using proxy by-pass sites or other means to subvert the filtering system	X						
Accidentally accessing materials that the school has agreed is inappropriate and failing to report it.	X						

Appendix 1

ICT Misuse/ E-Safety Breach Reporting Protocol



ICT misuse raised

Follow behaviour guidelines.

What type of activity is involved?

Illegal

Neither

Incident closed (is counselling or advice required? Does the policy need amending?

Inappropriate

Who is involved?

Child as instigator

Child as victim

Staff as victim

Staff as instigator

External instigator

Establish level of concern/ potentially inform parents/ E Safety lead/ SLT/record on CPOMS

Other children involved?

Potential legal or child protection issue?

If appropriate, disconnect, seal and store safely.

No

In school action*, designated safeguard leaders, eSafety Coordinator, SLT

Follow school's safeguarding procedures.

Advise person to contact police

Possible legal action

Yes

Counselling, monitoring, risk assessment

Maintain awareness of issue

School disciplinary and child protection procedures, possible parental involvement

Possible legal action

*Possible sanctions/actions (dependent upon level of concern)
-discussion with group of children/parents
-withdrawal of ICT privileges

Incident closed (is counselling/advice required? Does the policy need to be amended?)

Appendix 2

Acceptable Use Agreement for all Staff, Governors, Students, Parent Helpers and Volunteers

To ensure that staff and governors are fully aware of their professional responsibilities when using school's information systems, they are asked to agree to this code of conduct. Staff should consult the school's E-Safety policy for further information and clarification.

- The school's information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my school's information systems use will always be compatible with my professional role.
- I understand that the school's information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my school's information systems and Internet use to ensure policy compliance in accordance with the Data Protection Act.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school E-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will not use social media to communicate with pupils, parents/carers or ex-pupils on either the school's information systems, or personal systems/devices.

- I will promote E-Safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, and will delete any inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed ……………………………………………………………….

Name …………………………………………………………………. Date …………………………….

Appendix 3

STATHAM COMMUNITY PRIMARY

LYMM

Acceptable Usage Policy for using the Internet Statham Primary School

At School:

· We ask permission before using the computers, iPads or other electronic equipment.
· We are aware of and follow the SMART rules.
· We only view or delete our own work and not the work of other pupils.
· We only use websites or applications that an adult has chosen or that we think will help us with our work.
· We immediately close and report any webpage that we are not sure about.
· We tell an adult if we see anything we are uncomfortable with.
· We only e-mail other children in our school using DB primary when instructed by our teachers.
· We never give out personal information e.g.name, numbers or passwords.
· We never arrange to meet anyone we do not know.
· We do not open e-mails sent by anyone we do not know.
· We do not use social networking sites.
· We do not write, send or print any materials that are unfriendly.
· We always acknowledge materials that we have used from the internet.
· We do not use computers, mobile phones, iPads or other electronic equipment to hurt or upset other people.
· We will try to remember these rules when using computers, mobile phones or other electronic equipment outside school.

Outside of School:

· We will use the E-Safety skills that we learn in school to help us and others stay safe at home.
· We understand that any issues relating to E-Safety that occur at home could be dealt with within school, particularly if they involve our school or pupils.

I know that if I break any of these rules I may not be allowed to use any electronic devices within school.

Signed: ____________________

Appendix 4

Parent/Carers Internet Safety Agreement

Name of Child:________________________

As the parent/carer, I give permission for my child to use Statham's technology and devices.

I know that my child has signed an Acceptable Usage Agreement *and* has received guidance to help them understand the importance of online safety.

I understand that school will take reasonable precautions to ensure that my child will be safer when online, however, I understand that this manages risk but cannot eliminate it.

I understand that my child's online activity will be supervised and monitored and that school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I understand that the school will take appropriate action in the event of any incidents.

I will encourage my child to adopt safe use of the internet and digital technologies.

I will regularly visit the school’s website to keep up to date with any E-Safety news.

Signed:__________________________ Date: ________________