Little Stoke Primary School

E-Safety Policy

Review date – Nov 2016/Nov 2017

Next Review date – Nov 2018

Chair of Staffing & Curriculum Committee – Idara Udoh

Head Teacher – Scott Howes

Little Stoke Primary School
E-Safety Policy

Introduction
This policy aims to give all members of the school community clear guidance with regard to the rationale, principles, strategies and expectations of E-Safety at Little Stoke Primary School
Please read this policy in conjunction with our: Behaviour Policy, Child Protection Policy, Sex and Relationship Policy, Safeguarding Policy, Acceptable Use Policy and Staff Conduct Policy

Development, Monitoring & Review of this Policy
This E-safety policy has been developed by the Little Stoke Primary School E-Safety Committee:
Head Teacher (Scott Howes)
Deputy Head / E-Safety Officer (Anne Sargent)
Designated Safeguarding Leads (as above)
E-Safety Governor (Kirsty Wilmott)
Staff: including Teachers and Teaching Assistants
Integra technical support staff
Parent Representatives from parent contact group
School Council

Schedule for Development, Monitoring & Review

This e-safety policy was approved by the Governing Body:	27th November 2017
The implementation of this e-safety policy will be monitored by:	Head and Deputy Head / E-Safety Officer
Monitoring will take place at regular intervals:	September & February each academic year
The Chair of Governors / E-safety governor will be invited to review the implementation of the e-safety policy (which will include anonymous details of e-safety incidents) at the end of each academic year.	At least once a year
Should serious e-safety incidents take place, the following external persons / agencies should be informed as appropriate:	ART (Access and Response) LADO, Police

The school will monitor the impact of the policy using: Logs of reported incidents; Incident logs of internet activity (including sites visited); Internal monitoring data for network activity; Internet Surveys of Children, Parents/Carers & Staff twice a year.

Scope of the Policy
This policy applies to all members of the school (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.
The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but which are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

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 the internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school, nor the Local Authority can accept liability for the material accessed, or any consequence of internet access.

Roles and Responsibilities

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors reviewing information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor: Kirsty Wilmott

The role of the E-Safety Governor will include:

- Annual meetings with the E-Safety Officer
- Regular monitoring of e-safety incident logs
- Reporting to relevant Governors' meeting.

Head Teacher

- Has an overall duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer.
- 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.
- Are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- 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 those colleagues who take on important monitoring roles.
- Will receive annual monitoring reports from the E-Safety Officer.

E-Safety Officer

- Leads the e-safety committee which comprises of: Head, Deputy Head / E-Safety Officer, Designated Safeguarding Leads, E-Safety Governor, Kirsty Wilmott
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school technical staff from Integra traded services
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets annually with E-Safety Governor to discuss current issues, review incident logs, iboss and filtering/ change control logs.

The Network Manager (Integra) is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required e-safety technical requirements and any Local Authority Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- They keep 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 monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff are responsible for ensuring that:
- They have read, understood and signed the Staff Acceptable Use Policy (AUP) at the start of their contract.
- The accurate and timely record of their children's Acceptable Use Agreements are kept, and for ensuring copies are signed, dated and returned to the school office within the first 2 weeks of the academic year (or within 2 weeks of the child's start date).
- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They report any suspected misuse or problem to the Head Teacher, Deputy Head / E-Safety Officer for investigation.
- All digital communications with children/parents/carers should be on a professional level and only carried out using official school systems (e.g. not Facebook).
- Interactions on social media should not reference or discuss children, parents or school staff in any capacity where school matters are concerned.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Children understand and follow the e-safety and acceptable use policies.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where the internet is used, children should be guided to sites checked as suitable for their use.
- Processes should also be in place for dealing with any unsuitable material that is found in internet searches.

The Designated Safeguarding Leads will be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:
- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

The E-Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for annual reporting to the Governing Body.
Members of the E-safety Committee will assist the E-Safety Officer with:
- The production / review / monitoring of the school e-safety policy.
- Mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression.
- Monitoring network / internet / incident logs.
- Consulting stakeholders: including parents/carers and the children about the e-safety provision.
- Monitoring improvement actions identified through use of the 360 degree safe self-review tool.

Children
- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy**.**
- 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.
- 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 'in' and 'out' of school.

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/ mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school's Acceptable Use Policy, website and information about national/local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Their children's personal devices in the school (where this is allowed).

Policy Statements

Education for children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in e-safety is therefore an essential part of the school's e-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum should be provided as part of Computing/PHSCE/SRE/wider curriculum and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Children should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet is used, children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- In the unlikely event that inappropriate/unsuitable content is found/searched for on a device by a child, the child is explicitly taught to click on the Hector the protective dolphin and report the incident to an adult immediately.
- It is accepted that from time to time, for good educational reasons, children may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, the Head Teacher can request that the Integra Support team (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. The Head will email the technical support team to allow this to happen. Any request to do so, should be auditable, with clear reasons for the need.

Education for Parents and Carers

Parent/Carers play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Letters, newsletters, website.
- Parents/Carers E-Safety Workshops.
- High profile events/campaigns e.g. Safer Internet Day.
- Information about professional organisations such as CEOPs, Net Aware (NSPCC)

Education for Staff

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An informal audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training, the e-safety policy and procedures as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Officer will provide advice as required.

Education for Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are link governors for computing/e-safety/health and safety/child protection. This may be offered in a number of ways:

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

Technical: Infrastructure, equipment, filtering and monitoring

- 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 e-safety responsibilities.
- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/ security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school's infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Staff are made aware that removable media containing school data (e.g. memory sticks) must be encrypted 'in' and 'out' of school.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

- Children who bring their own mobile phone into school must leave it in the school office and collect it at the end of the school day. Children who bring in their own mobile phones, do so at their own risk.
- Any staff who BYOD must adhere to all elements of this policy. Mobile phones must be kept in lockers or locked in classroom cupboards. All cupboards have high bolts which should be used at all times. Mobile phones should never be used in the presence of children.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers, children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 children 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 in 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 children in the digital/video images.
- Staff and volunteers are allowed to 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.
- Care should be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Parents or carers will be given the opportunity to tell the school whether their child's photograph can be used when they fill in the school's registration form.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school data protection Policy is available from the school office on request.

The school will ensure that

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- It follows the LA Data Protection Policy.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

Staff must ensure that they

- At all times 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 data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, memory stick or any other removable media:
  - the data must be encrypted and password protected.
  - the device must be password protected
  - the device must offer approved virus and malware checking software.
  - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Communications

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and children or parents/carers (email, Twitter, social media 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.
- The contact detail on the web should be the school address, e-mail and telephone number. Staff or children's personal information will not be published, with teachers and teaching assistants only being contactable through: admin@littlestokeps.co.uk
- Whole class/group/individual email addresses may be set up and used for educational purposes.
- Children should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Social Media - Protecting Professional Identity & confidentiality

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

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

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

Unsuitable/inappropriate activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					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 school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						X
Creating or propagating computer viruses or other harmful files						X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
Use of social media on school equipment			X		X	
Use of messaging apps			X			
Use of video broadcasting eg Youtube			X			

Responding to incidents of misuse

This guidance is intended for use when Staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the website(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) for responding to online safety incidents and report immediately to the police.

Other Incidents

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

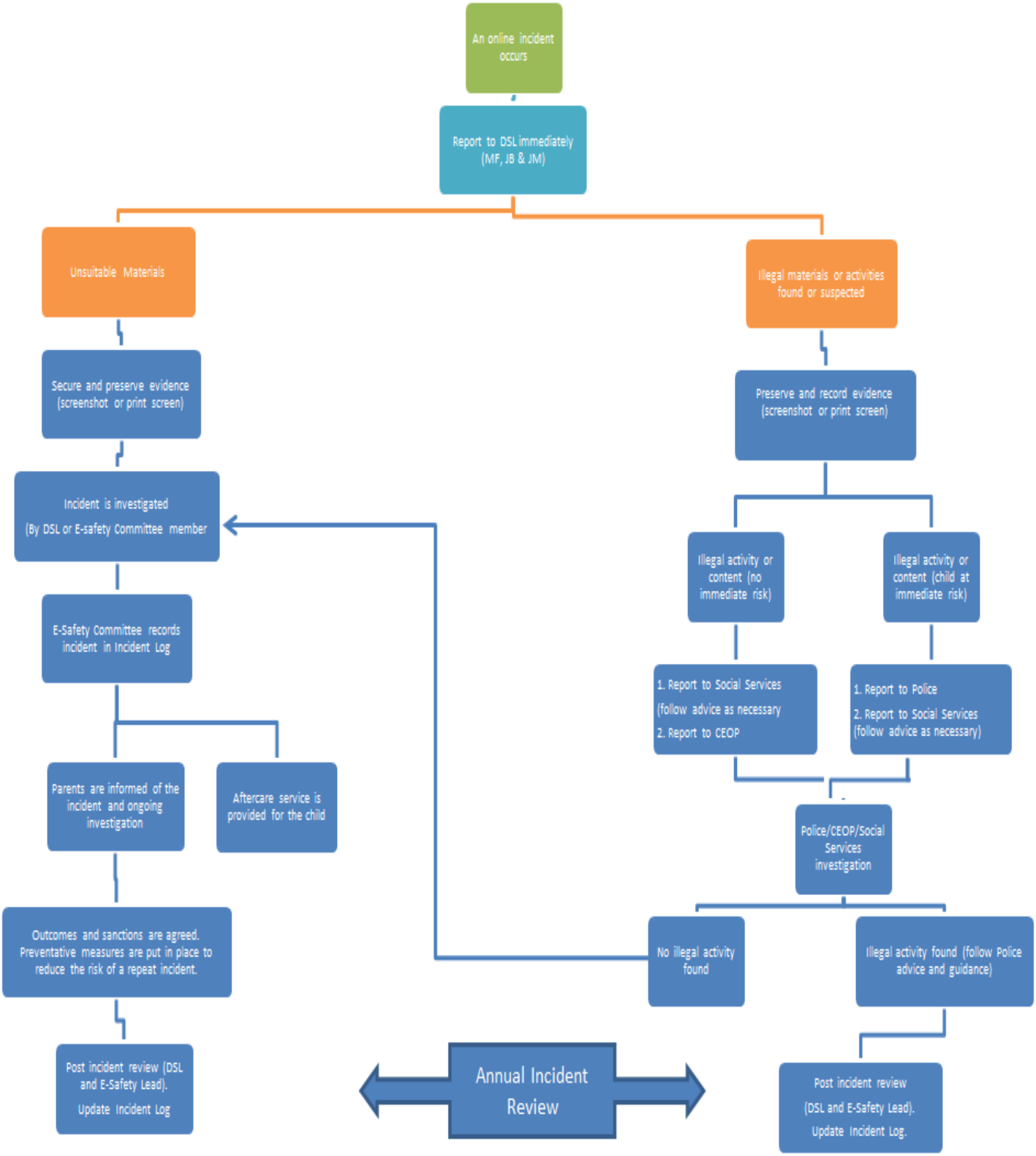
- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Record all evidence of the incident on the Yellow Welfare Concern Sheets to include:
  Name, Date, Class, Acceptable Use Policy, Details of the incident, Sanctions and Actions taken and parents informed column. These will be recorded onto CPOMS, our online safeguarding software.
- Inform Parents/Carers of any investigation that may involve their child, and update the Parents/Carers of any outcomes where legally entitled to.
- Ensure that the child's welfare, if involved in an incident, is at the forefront of any investigation. Preventative and educational measures should be implemented to minimise the risk of the same incident happening again in the future. Where any stress has been caused to the child (as a result of an online incident), the school will provide a counselling 'aftercare' service to help with the recovery for the child.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the 'url' of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority.
  - Police involvement and/or action.

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material or other criminally racist conduct, activity or materials.

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

Little Stoke E-Safety Reporting Flowchart



School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse when staff are using school equipment or BYOD on school premises. 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:

Incidents:	Refer to line manager	Refer to Head Teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X			
Inappropriate personal use of the internet / social media / personal email	X					X		
Unauthorised downloading or uploading of files	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		
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	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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
Using personal email/social networking instant messaging/text messaging to carrying out digital communications with pupils		X					X	X
Actions which could compromise the staff member's professional standing		X					X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	X
Using proxy sites or other means to subvert the school's filtering system	X				X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X		
Deliberately accessing or trying to access offensive or pornographic material		X			X		X	X
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following warnings		X					X	X

Appendices:

Pupil Acceptable Use Agreement (KS1)

Pupil Acceptable Use Agreement (KS2)

Little Stoke Primary School Key Stage 1

Dear Parent/Carer,

Little Stoke Primary School is committed to safeguarding and promoting the welfare of children. All pupils use computer facilities (including Internet access) as an essential part of their learning. Therefore, gaining pupils' and parents' agreement to e-safety rules is important.

Pupil's Agreement:

I agree to follow the SMART e-safety rules.

Name (PRINT): _____

Parent's Consent for Internet Access:

- I have read and explained the SMART e-safety rules to my child.
- I have read and understood the school e-safety rules and give permission for my child to access the Internet.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task.
- I will not take and then share online, photographs of other children (or staff) at school events without permission.

Name (PRINT): _____

Please sign here: _____ Date: _____

Be SMART – Stay safe on-line

Little Stoke Primary School – e-safety agreement

Safe	I won't speak to anyone about myself online.
Meeting	I won't meet anyone that I don't know.
Ask	I will always ask before I open anything I don't recognise. I will never open something I don't understand.
Remember	Don't go online without telling an adult first
Tell	I will tell a trusted adult if I see something I don't like or that makes me feel uncomfortable online. I will immediately click on the Hector the dolphin safety button

Little Stoke Primary School Key Stage 2

Dear Parent/Carer,

Little Stoke Primary School is committed to safeguarding and promoting the welfare of children. All pupils use computer facilities (including Internet access) as an essential part of their learning. Therefore, gaining pupils' and parents' agreement to e-safety rules is important.

Both pupils and their parents/carers are asked to sign this Acceptable Use Agreement to show that the e-Safety Rules have been read and understood. All children will have a laminated copy of this to refer to regularly

Pupil's Agreement:

I agree to follow the SMART e-safety rules.

Name (PRINT): _____

Parent's Consent for Internet Access:

- I have read and explained the SMART e-safety rules to my child.
- I have read and understood the school e-safety rules and give permission for my child to access the Internet.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task.
- I will not take and then share online, photographs of other children (or staff) at school events without permission.

Name (PRINT): _____

Please sign here: _____ Date: _____

Be SMART – Stay safe on-line

Little Stoke Primary School – e-safety agreement

These rules will help us to stay safe on the internet:

Safe — I will not chat or share personal information about myself (including photos) with online strangers.

Meeting — I will not meet (or attempt to meet) anyone that is a stranger to me online.

Accepting — I will not open any files, pop-ups or attachments that I don't understand or recognise.

Reliable — I understand that not all online information is true and reliable. I will always check the source of the information with a trusted adult.

Tell — I will tell a trusted adult if I see something that I don't like online and either use the Hector safety button or close my computer immediately. I will also tell a trusted adult if I feel I am being a victim of unkind or dangerous behaviour online.