Laurel Avenue
Community Primary School

Online Safety Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school Online Safety Policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and Governors to the classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

Internet use will enhance learning

- *The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils, provided through Durham ICTSS Broadband.*
- *Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Rules relating to safe internet access will be displayed alongside all computing devices throughout school.*
- *Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.*
- *Pupils will be shown how to publish and present information to a wider audience.*

Pupils will be taught how to evaluate Internet content

- *The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.*
- *Pupils will be taught the importance of cross-checking information before accepting its accuracy.*
- *Resources on the Thinkuknow website (www.thinkuknow.co.uk) will be used to teach pupils how to access the internet safely. These resources will be shared with parents through links on the school website and parents' meetings. Pupils will be taught how to report unpleasant Internet*

content e.g. using the CEOP Report Abuse icon or Hector Protector and by reporting to teachers in school.

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 Online Safety Policy is used in conjunction with other school policies (e.g. Behaviour, Anti-Bullying and Child Protection Policies). Alongside these policies, the school will refer to the 'Keeping Children Safe in Education' document – May 2016. However as with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

This Online Safety Policy has been developed by Laurel Avenue Online Safety Group made up of:

- *School Online Safety Co-ordinator*
- *Headteacher*
- *Deputy Headteacher*
- *Support Staff*
- *Governors*
- *Parents and Carers*
- *Community users*

Consultation with the whole school community has taken place through the following:

- *Staff meetings*

- *School Council*
- *Governors meeting/subcommittee meeting*
- *School website/newsletters*

Schedule for Development /Monitoring /Review

This Online Safety policy was approved by the Governing Body on:	
The implementation of this Online Safety Policy will be monitored by the:	*Laurel Avenue Online Safety Group is made up of:* ♦ *School Online Safety Coordinator* ♦ *Headteacher* ♦ *Deputy Headteacher* ♦ *Support Staff* ♦ *Governors* ♦ *Parents and Carers* ♦ *Community users*
Monitoring will take place at regular intervals:	*Annually:*
The School's Committee will receive a report on the implementation of the Online Safety Policy generated by the Online Safety Group (which will include anonymous details of Online Safety incidents) at regular intervals:	*Annually: Summer Term*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	
Should serious Online Safety incidents take place, the following external persons/agencies should be informed:	*LA Computing Manager, LA Safeguarding Officer, Police Commissioner's Office* *See Flow chart for all telephone numbers*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Surveys questionnaires of pupils*
- *Parents/carers*
- *Staff*

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the School's Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- *regular meetings with the Online Safety Co-ordinator*
- *regular monitoring of Online Safety incident logs*
- *regular monitoring of filtering/change control logs*
- *reporting to relevant Governors committee/meeting*

Headteacher

- *The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be shared with the Online Safety Co-ordinator*
- *The Headteacher is responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant*
- *There is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. All logs and minutes of meetings from Governors' Meetings and E Safety Group Meetings are logged. Support is offered by Headteacher and E Safety Co-ordinator and advice would be sought from Local Authority if appropriate.*
- *The Headteacher will work with the Online Safety Co-ordinator, regularly monitoring reports*
- *The Headteacher and the Deputy Headteacher should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff. (See flow chart on dealing with Online Safety incidents)*

Online Safety Co-ordinator

The Online Safety Co-ordinator works closely with Headteacher (also Child Protection Officer) to:

- *lead the Online Safety Group*
- *take day to day responsibility for Online Safety issues and have a leading role in establishing and reviewing the school Online Safety Policies/documents*
- *ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.*
- *provide training and advice for staff*
- *liaise with the Local Authority*
- *liaise with school ICT technical staff*
- *receive reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments (See Appendix 1)*
- *meet regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/ change control logs*
- *attend relevant meetings/committee of Governors*

Any investigation/ action/sanctions will be the responsibility of the Headteacher.

Managing the Network

The ICT Co-ordinator, with support from the ICT Technician and Headteacher, is responsible for ensuring:

- *that the school's ICT infrastructure is secure and is not open to misuse or malicious attack*
- *that the school meets the Online Safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance*
- *that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed*
- *the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- *that they keeps up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant*
- *that the use of the network/school systems/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Co-ordinator and Headteacher for investigation/action/sanction*
- *that monitoring software/systems are implemented and updated as agreed in school policies*

Teaching and Support Staff

The Teaching and Support Staff are responsible for ensuring that:

- *they have an up to date awareness of Online Safety matters and of the current school Online Safety Policy and practices*
- *they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)*
- *they have read, understood and adhere to the school's Social Networking Policy*

- *they report any suspected misuse or problem to the Online Safety Co-ordinator/Headteacher for investigation/action/sanction*
- *digital communications with pupils (email/school systems/voice) should be on a professional level and only carried out using official school systems*
- *Online Safety issues are embedded in all aspects of the curriculum and other school activities*
- *pupils understand and follow the school Online Safety and Acceptable Use Policy*
- *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*
- *they are aware of Online 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*

Child Protection Officer

The Child Protection Officer is trained in Online Safety issues and is aware of the potential for serious child protection 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*

Online Safety Committee

Members of the Online Safety Group will assist the Online Safety Co-ordinator with:

- *the production/review/monitoring of the school Online Safety Policy/documents*
- *the production/review/monitoring of the School Filtering Policy*

Pupils

All pupils:

- *are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (At KS1 it would be expected that parents/carers would sign on behalf of the pupils)*
- *have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations*
- *need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so*

- *will be expected to know and understand 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 Online Safety Practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school*

Parents/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, newsletters, letters, website/school systems and information about national/local Online Safety campaigns/literature.

Parents and carers will be responsible for:

- *endorsing (by signature) the Pupil Acceptable Use Policy*
- *accessing the school website/school systems in accordance with the relevant school Acceptable Use Policy*

Community Users

Community Users who access school ICT systems/website/school systems as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education : Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of the school's

Online Safety Provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- *A planned Online Safety Programme will be provided as part of ICT/PSHE and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school*
- *Key Online Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities*
- *Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information*
- *Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school*
- *Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet*
- *Rules for use of ICT systems/internet will be posted in all rooms and displayed on log-on screens where users agree or disagree on first log-in.*

- *Staff should act as good role models in their use of ICT, the internet and mobile devices*

Education: Parents/Carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- *Letters, newsletters, web site, school systems*
- *Parents evenings*
- *Reference to the SWGfL Safe website ("Golden Rules" for parents)*

Education : Extended Schools

The school does offer family learning courses in ICT, media literacy and Online Safety so that parents and children can together gain a better understanding of these issues. Messages to the public around Online Safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education and Training: Staff

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

- *A planned programme of formal Online Safety training will be made available to staff. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process.*
- *All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policies*
- *The Online Safety Co-ordinator will receive regular updates through attendance at training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and Professional Development days*
- *The Online Safety Co-ordinator will provide advice/guidance/training to individuals as required*

Training: Governors

Governors should take part in Online Safety training/awareness sessions, with particular importance for those who are members of the School's Committee and Online Safety Group. This may be offered in a number of ways:

- *Attendance at training provided by the Local Authority/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 Online Safety responsibilities:

School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the school's Security Policy and Acceptable Usage Policy and Durham Local Authority Online Safety Policy and guidance

- *There will be regular reviews and audits of the safety and security of school ICT systems*
- *Servers, wireless systems and cabling must be securely located and physical access restricted*
- *All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Co-ordinator and will be reviewed, at least annually, by the Online Safety Group*
- *All users (at KS2) will be provided with a username and password by the ICT Co-ordinator who will keep an up to date record of users and their usernames. Users will be required to change their password every term. Class log-ons and passwords will be used for KS1 and below. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access.*
- *The "master/administrator" passwords for the school ICT system, used by ICTSS and ICT Co-ordinator must also be available to the Headteacher or Deputy Headteacher and kept in a secure place; the school safe. Wireless Wep Key is also located in the school safe.*
- *Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.*
- *The school maintains and supports the managed filtering service provided by ICTSS*
- *Any filtering issues should be reported immediately to ICTSS.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager, Headteacher or Deputy Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Committee.*
- *Remote management tools are used by staff to control workstations and view users activity*
- *An appropriate system is in place for users to report any actual / potential Online Safety incident to the Network Manager (Headteacher/Deputy Headteacher). The incident is reported to the Network Manager (Headteacher/Deputy Headteacher) and logged on the incident record sheet. Sanctions are recorded in this policy clearing stating which incidences are deemed to be incidences and what the resultant sanction will be.*
- *Appropriate security measures are in place: County Filtering (internet), network security on server with administrative password, no remote services set up to the server so no one can access or attempt to access the school network. Wireless keys are set up which are secure and only known by a few personnel and locked inside school safe. These protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.*

- *An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system. 'Guests' will be given a log in – Supply1/Supply2/Supply3 with password of Password.*
- *An agreed policy is in place regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school. (see School Personal Data Policy for further detail)*
- *An agreed policy is in place (to be described) that allows staff to/forbids staff from installing programmes on school workstations / portable devices.*
- *An agreed policy is in place (to be described) regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school workstations/portable devices. (see School Personal Data Policy for further detail)*
- *The school infrastructure and individual workstations are protected by up to date virus software.*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See School Personal Data Policy Template)*

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum.

- *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.*
- *Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Co-ordinator (and Headteacher or Deputy Headteacher) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*
- *Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.*
- *Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.*

Use of digital and video images: Photographic, Video

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 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 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 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 (covered as part of the AUP signed by parents or carers at the start of the year)*
- *Pupil's work can only be published with the permission of the pupil and parents or carers.*

Data Protection

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 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 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:

- *the data must be encrypted and password protected*
- *the device must be password protected (many memory sticks/cards and other mobile devices cannot 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

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff and 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	√						√	
Use of mobile phones in lessons	√ *With permission*							√
Use of mobile phones in social time	√							√
Taking photos on personal mobile phones or other camera devices				√				√
Use of hand held devices e.g. PDAs, PSPs				√				√
Use of personal email addresses in school, or on school network		√						√
Use of school email for personal emails				√				√
Use of chat rooms / facilities				√				√
Use of instant messaging				√				√
Use of social networking sites				√				√
Use of blogs, e.g. school blog		√				√		

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. 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).*
- *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 pupils or parents/carers (email, chat, school systems 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 public chat /social networking programmes must not be used for these communications.*
- *Whole class or group email addresses will be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.*
- *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 should not be posted on the school website and only official email addresses should be used to identify members of staff.*

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

User Actions		*Acceptable*	*Acceptable at certain times*	*Acceptable for nominated users*	*Unacceptable*	*Unacceptable and illegal*
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	*child sexual abuse images*					√
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					√
	adult material that potentially breaches the Obscene Publications Act in the UK					√
	criminally racist material in UK					√
	pornography				√	

	promotion of any kind of discrimination				√	
	promotion of racial or religious hatred				√	
	threatening behaviour, including promotion of physical violence or mental harm				√	
	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				√	
Using school systems to run a private business					√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by ICTSS and or the school					√	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					√	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					√	
Creating or propagating computer viruses or other harmful files					√	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet					√	
On-line gaming (educational)		√				
On-line gaming (non-educational)					√	
On-line gambling					√	
On-line shopping/commerce					√	
File sharing					√	
Use of social networking sites					√	
Use of video broadcasting e.g. Youtube			√			

Responding to incidents of misuse

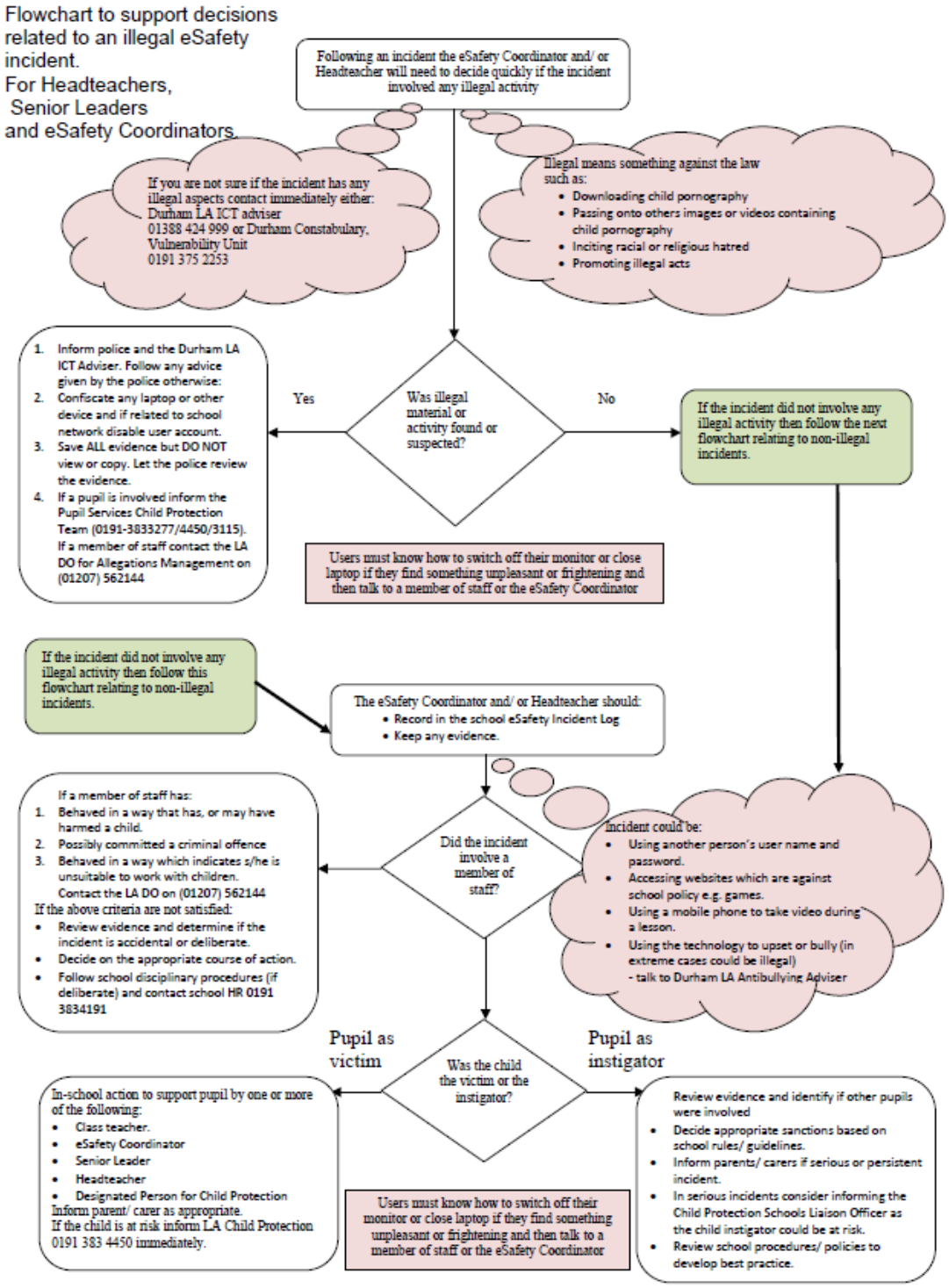
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through

careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- ***child sexual abuse images***
- ***adult material which potentially breaches the Obscene Publications Act***
- ***criminally racist material***
- ***other criminal conduct, activity or materials***

the flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event see Electronic Devices: Searching and Deletion Policy. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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:

Pupils ***Actions / Sanctions***

Incidents:	*Refer to class teacher*	*Refer to Deputy Headteacher*	*Refer to Headteacher*	*Refer to Police*	*Refer to technical support staff for action re filtering/security etc.*	*Inform parents / carers*	*Removal of network / internet access rights*	*Warning*	*Further sanction e.g. detention/ exclusion*
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√	√	√	√	√	√	√
Unauthorised use of non-educational sites during lessons	√	√	√		√	√	√	√	
Unauthorised use of mobile phone / digital camera / other handheld device	√	√	√			√	√	√	
Unauthorised use of social networking / instant messaging / personal email	√	√	√		√	√	√	√	
Unauthorised downloading or uploading of files	√	√	√		√	√	√	√	
Allowing others to access school network by sharing username and passwords	√	√	√			√	√	√	
Attempting to access or accessing the school network, using another pupil's account	√	√	√			√	√	√	

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

Staff

Incidents:	*Refer to Headteacher*	*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).	√	√	√	√	√	√	√
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	√				√		
Unauthorised downloading or uploading of files	√				√		
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	√	√			√	√	√
Careless use of personal data e.g. holding or transferring data in an insecure manner	√				√		
Deliberate actions to breach data protection or network security rules	√	√	√	√	√	√	√
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	√	√		√	√	√	√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√		√	√	√	√
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	√	√	√	√	√	√	√
Actions which could compromise the	√	√	√	√	√	√	√

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

Signed: K Hodgson
Coordinator
Date: June 2017

Signed: N Dixon
Chair of Learning, Teaching and Achievement Committee
Date: June 2017

Date of Policy: June 2017
Date of Review: June 2020

Appendix 1: Online Safety Incident Log

Appendix 2:

Keeping Children Safe in Education – May 2016

Appendix 3: Useful resources for teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Becta
http://schools.becta.org.uk/index.php?section=is

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

Kent Online Safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/Online Safety home.cfm

Kidsmart
www.kidsmart.org.uk/
Kent Police – Online Safety
www.kent.police.uk/Advice/Internet%20Safety/Online Safety%20for%20teacher.html

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 4: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Kent leaflet for parents: Children, ICT & Online Safety
www.kented.org.uk/ngfl/ict/safety.htm

Kidsmart
www.kidsmart.org.uk/

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.co.uk
Think U Know
www.thinkuknow.co.uk