On-line SAFETY POLICY

Produced by: Mr Tom Arnold
Reviewed by: SLT

Published: Sep 2016
1st Review Date: January 2017

Contents

Appendicies

1.0 Rationale and Purpose

E-Safety encompasses Internet technologies and electronic communications such as mobile smartphones, games consoles with Wi-Fi capabilities, as well as collaboration tools, such as our VLE, and both pupils and staff using computers at home. It highlights the need to educate pupils about the benefits and risks of using technology, and provide safeguards and awareness for users to enable them to control their online experience. The school recognizes that pupils, staff and stakeholders of all varieties have personal devices not owned or covered by the school. People should be taught and encouraged to consistently make informed and sensible decisions for themselves. E-safety is not just about rules and forming a water tight policy considering every eventuality; because the emphasis is on ensuring that all stakeholders UNDERSTAND THE RISKS in all situations and act accordingly.

Education on managing these risks is every bit as important as forming and following rules and regulations, if not more so. This ensures that when new technologies emerge and new hazards are identified, everyone has the correct mindset to manage the the emerging hazard, and is already protected by the depth of their existing, savvy understanding of e-safety.

For succinctness and ease of use, this policy has been refined to this document, with all supporting appendices stored separately.

Naturally, this policy is subject to amendments, as are the Acceptable Use Agreements signed by staff and pupils. These represent all fundamental rules and stipulations.

The school's e-safety policy will operate in conjunction with other policies including those for Good behaviour, Photographing of children, Curriculum, Child protection, Anti-bullying, Data Protection and Security.

2.0 Understanding the Risks

2.1 Teaching and Learning Using the Internet

UNDERSTANDING THE RISK – Pupils could intentionally or inadvertently access inappropriate internet content. The main areas of concern are: violence, 'adult' content/nudity, bias and discrimination. This content could take the form of text, images or videos. Pupils could find this content distressing, misleading, worrying or frightening etc. Potentially, the internet could be searched by one pupil and these findings, viewed by another, therefore pupils are dependent on safe use from their peers for protection.

2.2 Managing Information Systems

UNDERSTANDING THE RISK – Viruses and inappropriate access are a hazard to our school's servers and internal systems. A security breach or virus attack could result in the failure of our systems, the loss or leakage of confidential pupil information and the loss, hijacking or theft of files saved by teachers and pupils throughout the school.

2.3 Protecting Personal Data

UNDERSTANDING THE RISK – The school holds data and information regarding pupils and teachers that is highly confidential. Details include, pupils' dates of birth, addresses and attainment grades. Leakage of data such as this could compromise children. In a worst case scenario, a data leakage could lead to 'predators' accessing information about a child's locality, which is of course a Child Protection issue so data confidentiality and security are paramount priorities.

2.4 Managing e-mail

UNDERSTANDING THE RISK – e-mail when used unsafely represents a threat to teachers and pupils. If the confidentiality of a password is broken then private e-mails, which that e-mail account holder has sent and received can be read and printed by others. Also e-mails can be sent from an account that have not been written by the account holder. Potentially, a teacher could have an incriminating e-mail maliciously sent from their account by a pupil or other body. Pupils can also be potentially reached through e-mail for 'grooming' purposes.

2.5 Managing Social Networking, Social Media and Personal Publishing

UNDERSTANDING THE RISK – social networking is possibly the area of highest risk for all who use websites such as Twitter, youtube or Facebook. For staff, there are many possible areas of concern including: identity theft, disclosure of personal information that one may wish to keep private e.g.: religion or date of birth and the publication of embarrassing or even incriminating photographs. Careers in education have been ended through mistakes made using social networking sites or by using them to slander individuals or management within schools. As well as the hurt caused to individuals, this can be highly damaging to the school's reputation. For pupils the risks with these sites are primarily of damages to self-esteem, vulnerability to 'grooming' and of being victims or perpetrators of cyber bullying. Cyberbullying is the use of ICT facilities for slander, accusation, humiliation, threat or any other form of emotional assault.

Just a few of the examples of cyberbullying include; having a facebook conversation in which someone is insulted; the creation of a facebook group titled 'Joe Bloggs is a loser,' or similar; the sending of either open or anonymous e-mails, facebook or text messages that are threatening, defamatory, profane or insulting; behaving in a similar way across X-box live; or the creation of a website which pokes fun at a person or group**.**

2.6 Managing Learning Platforms and Learning Environments

UNDERSTANDING THE RISK – Learning platforms are an emerging new technology. Great care must be taken when rolling them out because of the risks involved. Pupils could potentially have access to school data and resources outside of school. If they have a school e-mail address then the school may be accountable for e-mails sent by pupils whilst not supervised by staff. Teachers and pupils could potentially have contact out of school. Assessment of these risks is an essential part of deciding exactly what form any learning platform use will take, and what levels of access different groups of people will have i.e.: school leaders, teachers, teaching assistants, pupils and parents.

2.7 Photographing children safely

UNDERSTANDING THE RISK – Images of children need to be treated with great care, especially if pupil's names are attached to the image. Pupils have a right to the privacy of any pictures that are taken of them, and any unauthorised dissemination of images is a violation of children's rights. In other schools, predatory individuals have been known to use a named photograph of a child to approach them in the street, then address them by their name in an attempt to gain their trust.

2.8 Authorising Internet Access

UNDERSTANDING THE RISK – Internet access in schools is something which parents have authority over. Parents' permission must be formally obtained before any pupil accesses the internet. The school is fully liable if this process is not followed. Pupils have the right to feel safe using the internet, so pupils who deliberately break e-safety rules are a potential threat to others.

2.9 Using the Internet Outside of School

UNDERSTANDING THE RISK – Pupils are at risk when they use technology outside of school. There is a danger that pupils could follow rules in school, but unless they are able to make informed, responsible decisions outside of school they could be in danger to the full spectrum of e-safety hazards.

2.10 Introducing the Policy to Pupils

UNDERSTANDING THE RISK – If all pupils are not clear exactly what our rules are then they are at risk from all hazards mentioned hitherto in this policy. The main areas of risk are; accessing inappropriate internet content, being victims or perpetrators of cyber bullying, disclosing personal details, using images of themselves unwisely. The most concerning risk of all is that of vulnerability to predatory individuals.

2.11 Teaching Pupils to be e-Safe at Home

UNDERSTANDING THE RISK – Pupils use of the internet at home is well beyond the jurisdiction of the school. This means that pupils can be at risk from all possible threats mentioned hitherto, potentially far more so. In school, web content is filtered and screened by KCN, where as at home there is potentially no filtering at all, giving pupils unrestricted access to the entire scope of the internet – the vast majority of which is intended for adults. Furthermore, if pupils do not fully understand the reasons for e-safety rules in school, then they may be inclined to ignore these safe practices at home. Worst case scenario is that a pupil could meet unaccompanied someone in the real world, that they have previously only met on line.

2.12 Enlisting Parents' Support

UNDERSTANDING THE RISK – Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology with tablets and smartphones. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home and in all other areas outside of school e.g.: libraries, internet cafes etc. They could therefore be using technology safely at school but not beyond this, so working together with parents is a vital part of keeping children e-safe.

2.13 Discussing the Policy with Staff

UNDERSTANDING THE RISK – All staff need to know what the risks are throughout the full arena of e-safety. Without comprehensive awareness of the risks and corresponding rules and safe practices, teachers are likely not to be e-safe themselves, nor be in a position to educate the pupils in their care. This unacceptable situation would represent a direct risk to staff and pupils' safety and security.

2.14 Ofsted categories of risk.

Annex 4. Content, contact and conduct exemplars[17]

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	advertisements spam sponsorship personal information	violent/hateful content lifestyle sites	pornographic or unwelcome sexual content	bias racist misleading information or advice
Contact (child as participant)	tracking harvesting personal information	being bullied, harassed or stalked	meeting strangers being groomed	self-harm unwelcome persuasions
Conduct (child as actor)	illegal downloading hacking gambling financial scams terrorism	bullying or harassing another	creating and uploading inappropriate material; sexting	providing misleading info and advice health and wellbeing; time spent online

3.0 Policy

At Salmestone we have produced an e-Safety policy that replaces the Internet Policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

The policy is being generated as of January 2014, by Tom Arnold, ICT leader and e-Safety officer, parents, the governing body, teachers, the school council and the senior leadership team.

The head teacher and the ICT co-ordinator work together on issues regarding e-safety. Our e-Safety Policy has been written by the school, building on the KCC e-Safety Policy and government guidance. It has been agreed by the senior leadership team and approved by governors. The e-safety Policy and its implementation will be reviewed annually. Procedure for all e-safety incidents and breaches of policy are governed by the highly visible flow charts. (see flow charts.) The attention of all staff is drawn to these and all other aspects of e-the school's e-safety policy through professional development and at induction.

Aims
At Salmestone we aim to:

- Provide a safe and secure environment for learning, in all risks are managed. This includes learning with information systems and electronic communications.
- To protect pupils from unsuitable materials published on the internet.
- To provide pupils with current and up to date technology in preparation for life and future work.
- To ensure pupils are aware of the risks involved and the right choices that will help keep themselves safe when using information systems and electronic communications. They need to be made aware of the best and worst case scenarios when managing risks both at school and at home.
- To tackle cyberbullying in line with the school's anti-bullying policy.

Teaching and Learning
At Salmestone we believe that the purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management function. It is always used with our vision in mind. Internet use is also part of the statutory curriculum and a necessary tool for learning. The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality, managed and guided internet access as part of their learning experience. Pupils use the internet widely outside school and need to learn how to evaluate internet risk and to take care of their own safety and security.

The benefits of using the internet in education include:

- Access to world-wide educational resources;
- Inclusion in the National Education Network which connects all UK schools;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Access to learning wherever and whenever convenient.
- Educational and cultural exchanges between pupils world wide.
- Access to experts in many fields for pupils and staff.
- Collaboration across support services and professional associations.
- Exchange of curriculum and administration data with KCC and DfES.

The school internet access is designed expressly for pupil use and includes filtering appropriate to primary aged children. Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils are reminded of how to use the internet safely on a regular basis, during the ICT curriculum for the first term of every year.

They are to be made aware of all risks. This is also to be reinforced during an e-safety day, in which an annual competition for the 'keeping Salmestone e-safe' posters is undertaken through assemblies. Internet access is planned to enrich the curriculum and extend learning opportunities. Staff guide pupils in on-line activities that support planned learning outcomes. Pupils are supervised at all times whilst using the internet. Teachers are urged to conduct image searches before lessons to vet results away from the presence of pupils.

The school ensures that the copying and subsequent use of internet derived materials by staff and pupils comply with copyright laws. Pupils are taught to acknowledge the source of information used and to respect copyright when using internet materials in their own work in the e-safety curriculum.

Managing Information Systems

Local Area Network Security:
Users must take responsibility for their network use. For KCC staff, flouting electronic use policy is regarded as a matter for dismissal. Servers are located securely and physical access is restricted. At Salmestone we employ Centaur Systems to keep the server operating system secure and up to date, with current virus protection for the whole network and they pro-actively manage access by wireless devices to the network.

Wide Area Network (WAN) Security:
All internet connections are arranged via the Kent Community Network to ensure compliance with the security policy. KCN firewalls and switches are configured to prevent unauthorised access between schools. Decisions on WAN security are made on a partnership basis between school and KCN.

The security of the school information system is reviewed regularly and virus protection is updated regularly. Personal data sent over the Internet will be encrypted or otherwise secured. Files held on the school's network are checked regularly. The ICT co-ordinator and the network manager review system capacity frequently.

E-mails
Staff and pupils may only use approved e-mail accounts. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils are taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. Whole class e-mail addresses are used for pupils at Salmestone Primary School to communicate with others outside of school and an internal message/email programs can be used for pupils to contact each other in school.

E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written in school headed paper. The forwarding of chain letters is not permitted.

The contact details on the website are the school address, e-mail and telephone number. Staff and pupils' personal information is not published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website complies with the school's guidelines for publications including respect for intellectual property rights and copyright.

Website
Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. They are to be facing away from the camera. Pupils' full names are not used anywhere on the website and their faces are not to be shown. Written permission from parents or carers is obtained before images of pupils are electronically published. Work is only published with the permission of the pupil and parents.

Social Networking
Pupils are advised never to give out personal details of any kind that may identify them and / or their location. Examples include real names, address, mobile and landline phone numbers, school attended, e-mail addresses, full names of friends, specific interests and clubs. Pupils are advised not to place personal photos on any social network space. The school filters access to social networking sites. Pupils have been advised not to use social networking sites until KLZ is available. Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. The school is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments. As social network sites such as Facebook and Bebo should not be available to Primary aged children, they are strongly advised not to engage in these activities.

Nonetheless, pupils are to be advised that to take safety measures such as keeping personal information private and using the site's own safety settings correctly. In year 5 and 6 pupils are given specific lessons on how to use facebook and similar sites safely, with regard to vulnerability to predators, as well as their general emotional well-being.

Filtering
KCN filter the internet that is received by Salmestone Primary School. These blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking lists is a major task as new sites appear everyday. The school works with KCC and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.

If staff discover unsuitable sites, they are to follow the relevant flow chart to manage the issue. Ultimately the URL must be reported to the e-Safety officer, who will report the site to the relevant filtering agency eg: analysis team from EiS. These can be reported via the technicians. The ICT Leader works with the technicians and EiS to follow all recommendations and handle queries regarding filters.

Videoconferencing and video sites.
All videoconferencing equipment in the school is switched off when not in use and not set to auto answer. Pupils ask permission from the supervising teacher before making or answering a videoconferencing call. Videoconferencing is always supervised by a school member of staff. When recording a videoconferencing lesson, written permission is requested by all sites and participants. The reason for recording must be given and the recording of all videoconferencing should be clear to all parties at the start of the conference.

Youtube.com is a website which brings often incomparable benefits for education, but unfiltered access brings an unacceptably high level of risk, considering youtube's content. Therefore the education video website is to be used as it is specifically designed. If staff wish an education video to be made accessible on this site, for the purposes of showing children, then they are to request it. The turnaround speed for such requests is to be monitored by the e-safety officer.

VLE
The VLE employed by Salmestone Primary school is to be managed by the ICT leader in their role as e-safety officer. He is responsible for managing its internal flagging system, following up flagged incidents and for advising pupils as to its use. He is responsible for showing pupils how to use the 'flag to admin' button as a call for help. He is also responsible for reassuring pupils who have used the system and for disciplining offending pupils, in accordance with the schools behaviour policy. An entry is always to be made into the school's e-safety log.

As the use of this technology expands, pupils and adults shall be mindful of all dangers emerging in all 6 areas of risk, manage them accordingly and adapt this policy as necessary.

Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions
The school maintains a current record of all staff and pupils who are granted access to the school's electronic communications. All staff are required to read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.

Pupil access to the internet will be by adult demonstration, followed by supervised access to specific, approved on-line materials. Parents are asked to sign and return a consent form for pupil access.

Internet Access

The school maintains a current record of all staff and pupils who are granted access to the school's electronic communications. All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource. At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. At Key Stage 2, pupils have a little more access to internet use but must use search-engines that have already been approved from a favourites list and the e-safety posters.

The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use. The school audits ICT use to establish if the e-safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

E-Safety Complaints/Incidents and Procedure of Concern

If a pupil finds an inappropriate/offensive website the pupil should click 'Hector Protector' to blank the screen from themselves and others immediately. Once the children are away from the situation please note the web address/URL and report it immediately to the SLT of ICT Co-ordinator. They will report this to the internet filtering service – KCN. A member of SLT will inform the parent/carer of the incident, how it came about and the action taken. An entry is always to be made in the school's e-safety log which is kept in the ICT suite. For further details see the schools flow charts.

Incident management

The following is an example of how an incident, such as a Cyberbullying issue, would be dealt with:

- The evidence is examined by the e-safety officer.
- If the complained is viable, the victimised parties are to be reassured and the offending parties investigated. The headteacher is informed.
- Once guilt has been established, the offenders are strongly spoken to.
- "Lets look at the cyberbullying wheel and look at the bad choices you've made."

- If people gang up and are repeatedly unkind then this is bullying behaviour.
- “Do you really want someone in your class in tears and afraid to come to school?”
- All parties should be using all forms of the internet in the main room of the house, accompanied by their parents/guardians.
- “You can be reported to Moderators for this kind of behaviour.”
- “The police can arrive at your front door if you are over 10.”
- The rude things in class and on line need to stop immediately.
- “I am coming to talk to the whole class to emphasise only talking to people you know, telling me if someone is being unkind to you and using the console in the front room of the house.”
- “Ill let The Headteacher decide whether or not we to speak to your parents/guardians.”

The e-safety officer is then to monitor the situation by asking the offended parties after a few days and weeks if the situation has been resolved. An entry is to be made into the e-safety log. The e-safety officer then advises the victimised party as to how young people can best be protected from cyberbullying:

- The importance of using all internet based activities in the front room of the house for the child’s supervision and protection.
- Does the child know the people that they are talking to online? They should only be communicating online with people that they know in the real world already.
- Offenders who are not members of our school, need to be reported to the platform’s moderators, or the police. The e-safety officer will monitor the outcome.
- The victim is invited to keep us informed about the situation and to report back to us in a few weeks. If they are still being bullied then further drastic action is taken. The headteacher will decide if the police need to be informed.

  Any complaints about staff misuse, or breaching of the acceptable use agreement must be referred to the head teacher. The e-safety leader may be requested to assist with investigations.

  Any pupil that receives unpleasant VLE messages is told to use the internet ‘Flag to admin’ button to report it to the e-safety officer. The VLE message will then be investigated in a similar manner to the above, and the offending user personally warned in the first instance. If a pupil persistently offends then they are blocked whilst their parents/carers are informed and the matter is discussed with them.

The Policy and Pupils

E-Safety 'keeping Salmestone e-safe' posters are posted in all rooms where pupils have internet access and pupils are informed that network and internet use is monitored. Pupils are to be questioned about these and asked about them as a means of evaluating their impact. The importance of E-Safety is discussed on a regular basis to raise the awareness and importance of safe and responsible internet use. An E-Safety module will be included in the PSHE and Citizenship programmes covering both school and home use.

The school council is involved in evaluating the 'keeping Salmestone e-safe' poster on an annual basis. Any changes involve necessitate an update in the school's disseminated posters. This is seen as an opportunity for further pupil involvement as a new competition for their final design/style is then run.

Pupils' e-safety work is displayed in the ICT suite.

An assembly is run by the e-safety officer for Key stages 1 and 2, three times a year, including on National internet safety day.

The Policy and Staff

All staff are given the School E-Safety Policy and its application and are made aware that Internet traffic can be monitored and traced to the individual user, which is furthermore explained in the Acceptable use agreement. Discretion and professional conduct is essential. Staff training in safe and responsible Internet use, all six key areas of risk and on the school E-Safety Policy is provided as required, on an annual basis, with updates given as necessary. Staff are shown how to use the p's: 'print screen, open Paint, paste and print' to capture any screen as it exists. All teaching and support staff sign an acceptable use agreement. All further staff e.g. mid-day meal supervisors and cleaners are to be involved in e-safety to the following level: They are to be alert and aware for any sign of e-safety danger, as they would for any health and safety risk. Should they see anything that goes against the keeping-Salmestone e-safe posters e.g.: an inappropriate digital photograph or web-site print-out, pupils using a computer at lunchtime apparently unsupervised, or a disclosure of cyber-bullying, then are to ask the school office to alert me as soon as possible. New members of staff are given training on the policy, the Acceptable use agreement they are to sign, the e-safety posters, the flow charts and the e-safety log.

The e-safety officer may be required to liaise with other schools and personnel within T-Kat.

The Policy and Parents

Parents' attention will be drawn to the school's e-safety policy in newsletters, the school website and the school prospectus. Internet issues will be handled sensitively, and parents will be advised accordingly. Parents are invited to comment on the e-safety policy and provide suggestions as to its development annually via the school's website. Advice and recommendations are to be as up to date and widespread as possible, covering all aspects of e-safety. The following strategies are to be used to communicate key aspects of the policy and to provide guidance for parents as to how to best keep their children safe, savvy and alert to the risks when going on-line:

- Open even sessions are to be offered, led by the e-safety officer and the Family liaison Officer.
- Also, there will be drop in morning sessions at 9:00 am with tea and coffee. The e-safety officer and Family liaison officer combine their expertise to hold these sessions for parents. They can bring in their laptops, tablets, smartphones etc. so that we can show them how to set up different accounts for different family members and install the correct safety features, filtering and parental controls, including those pfovided by Apple and Microsoft.
- Parents are requested at all sports days and performing activities not to publish any photos or videos of children, as they may well show other children, which is Illegal (Data protection act 1998) as parental/carer permission has most likely not been given. They are to be reminded that the school has many Looked after children for whom staff are not allowed to be photographed at all.
- The school is to use social media as a communication tool by setting up a facebook page and Twitter account, probably under the banner of: Salm-e-safety.
- The school will have a section of its website which will be a comprehensive one-stop-shop for all aspects of e-safety hosting:
- Links to the latest government, ceop and childnet advice,
- Links to child friendly e-safety resources such as the cybercafé and the cbbc e-safety feature.
- the ceop button as a reporting mechanism and urgent call for help if people suspect their child is being groomed.
- A message box which enables adults to message me with any queries about e-safety.
- A breakdown of all e-safety issues in the form of a T diagram with the risks on one side and the solutions on the other.
- Links to the official family safety pages from Microsoft and apple.
- A jargon/acronym breakdown, CEOP, URL, WWW, etc.
- Games and interactive features.

- This page will also include information on video gaming systems and the importance of the PEGI age-rating system, such as a copy of FLO's latest leaflet.
- Finally, a link to Mr Arnold's e-safety blog.

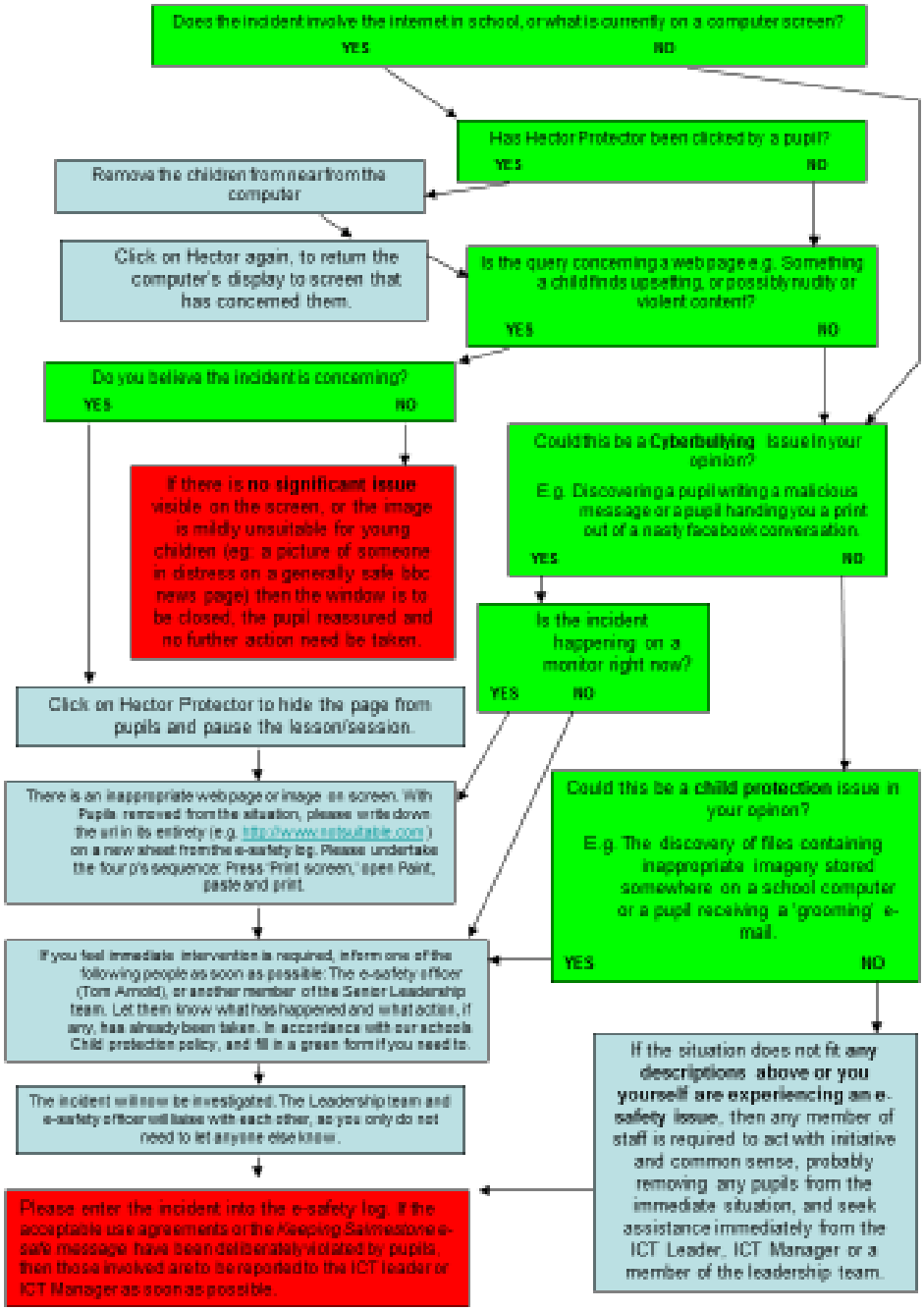
SIGNED: _____ DATE: _____

PRINT NAME: _____

APPENDICIES

3.1 What do I do if I directly encounter an e-safety issue?

What do I do if I directly encounter an e-safety issue?



4.0 Ofsted expectations and questions

The latest report had a number of key findings:

- In the five schools where provision for e-safety was outstanding, all the staff, including members of the wider workforce, shared responsibility for it. Assemblies, tutorial time, personal, social, health and education lessons, and an age-appropriate curriculum for e-safety

all helped pupils to become safe and responsible users of new technologies.

- Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.
- In the outstanding schools, senior leaders, governors, staff and families worked together to develop a clear strategy for e-safety. Policies were reviewed regularly in the light of technological developments. However, systematic review and evaluation were rare in the other schools visited.
- The outstanding schools recognised that, although they had excellent relationships with families, they needed to keep developing these to continue to support e-safety at home.
- Few of the schools visited made good use of the views of pupils and their parents to develop their e-safety provision.
- In some schools there were weaknesses in e-safety where pupils were receiving some of their education away from the school site.
- The weakest aspect of provision in the schools visited was the extent and quality of their training for staff. It did not involve all the staff and was not provided systematically. Even the schools that organised training for all their staff did not always monitor its impact systematically.

Recommendations for schools

The report recommended that schools:

- Audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- Work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- Use pupils' and families' views more often to develop e-safety strategies
- Manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school
- Provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- Work with their partners and other providers to ensure that pupils who receive part of their education away from school are e-safe

- Systematically review and develop their e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding.

PUPIL QUESTIONS

- If you felt uncomfortable about anything you saw, or if anybody asked you for your personal details such as your address on the internet would you know where to go for help?
- If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?
- Can you tell me one of the rules your school has for using the internet?
- Can you describe the risks of posting inappropriate content on the internet?

5 .0 e-safety curriculum

Salmestone Community Primary School e-safety curriculum

General points

1. E-safety is to be introduced at the start of the year, so that children can use the resources in school (including cameras) safely. This is then followed up by an e-safety unit in them three (wave two)
2. This curriculum is structured in this way (Primarily by theme) so that each year revisits and builds upon previous learning.
3. The ICT leader will manage the use of the school's shared area and to support e-safety

Theme 1 of 4 – Computer use in school – term 1 and 3

	Learning Outcomes	Suggested activities
R	If pupils see anything which they find inappropriate or upsetting then they should click on HECTOR PROTECTOR who will cover their screen.	Discussing what things on the internet can be frightening. Drawing a picture of HECTOR and writing/talking about how he helps look after us. Practice using Hector protector
1	Pupils learn that we can only use the internet when supervised by an adult. Pupils learn the Bee safe poster for KS1 and the reasons behind it.	Discussion of why we need our e-safety posters using : http://www.thinkuknow.co.uk/5_7/leeandkim https://www.thinkuknow.co.uk/Teachers/Lee-And-Kim/ Singing Superhero Sid's music video.
2	Recap of year 1. Pupils also learn that they can only do a search iusing a safe search engine.	http://www.thinkuknow.co.uk/5_7/hectorsworld/ Recap Singing Superhero Sid's music video, watch Lee and Kim's animal adventures (from shared area) and read and discuss his top tips. Pupils learn KS1 Bee safe poster and reasons behind it. Pupils make e-safety poster
ALL KS2	Pupils are to be taught that search engines such as google are not safe as they do not always give results that we want to see. We explain to pupils that the results of this search engines are not always safe. We warn pupils that if we are not careful we will accidentally find things that are unsuitable for our age, which can be very frightening and upsetting.	Pupils are to be consistently reminded of the reasons WHY we need to follow the 'Keeping Salmestone e-safe' poster for juniors. PUPILS FROM YEAR 4 ONWARDS ARE TAUGHT THE MEANING OF THE SALM-E-SAFETY POSTERS AS DESIGNED BY LR in term one PUPILS ARE TAUGHT THE ACCEPTABLE USE AGREEMENT in term 3 All PUPILS UNDERTAKE A CHOICE WHEELS activity in in term 3
3	Pupils learn the Keeping Salmestone e-safe poster for KS2 and the reasons behind it. Pupils are taught to be careful in all the choices they make with regard to using the internet. Pupils are to be taught that they are not to deliberately search for rude/violent/inappropriate things. They need to know that if they are irresponsible in their internet use then they are risk having their license to use the internet revoked, and their log on details blocked. Pupils are introducted to the VLE. They are to be made aware of the need for confidentiality of their password, and that the content of all their messages is monitored. They are to be informed of the flagging system.	http://www.thinkuknow.co.uk/5_7/hectorsworld/ Cartoon 1 which covers the dangers of disclosing personal information. Cartoon 6 which covers cyberbullying. (ICT leader to use VLE to provide parents and pupils with inks for the page, so that all cartoons can be viewed from home.) Video and game certificates discussed. Discussion of the message behind each of the videos. Followed by activities such as reading the story in pdf format – see shared area. Pupils learn to only use the internet when supervised. Learn first parts of e-safety agreement. Discussion of worst case scenarios. (see: Understanding the risks throughout e-safety policy) Pupils undertake 'Jigsaw' activity where pupil revise from last year: Full set of six wheels. where they are required to match the risks to the best and worst case scenarios, showing the different possible consequences of their choices. These wheels are to be displayed in the ICT suite afterwards. Emphasis made on the words 'risk' and 'choice' throughout.

		Use: cyberbullies; predators; inappropriate content. Draw a storyboard cartoon of someone making the right choice, possibly using laptops and the program '2simple to create a story in purple mash' Interactive demonstration of the VLE's flagging system for messages. During assembly Mindmap cyberbullying forms to know what they are. Undertake safe research
4	Recap all of year 3. Pupils are advised that even if they think they are 'not scared of anything' pupils need to be considerate of friends. Data protection is taught so that pupils know the reasons why they cannot access other people's files at school. Pupils will be taught to acknowledge the source of information used and to comply with copyright legislation	Choice wheels activity: 3 of 6 to be used, revising last year Pupils design a flow chart diagram of data protection showing data being taken down a dangerous path eg: a cedit card number emailed from, for example, a dad to his daughter who s on holiday in Australia except Dad mistypes the email address and it goes to a hacker Pupils learn 4 ps sequence and flag to admin. Watch 'cyberbullying virus' video on youtube. Pupils learn the need Full mindmap of cyberbullying. Negative feelings it can cause, methods of bullying, Research e-safety using salmeston-line
5	Recap of year 3 and 4. Pupils must be reminded to be responsible and savvy in their searching and the choice they make with each click. They are to be aware of the risks involved in 6 key areas of e-safety: 1) Predators 2) Viruses and malware 3) Hackers and data theft 4) Inappropriate internet content 5) Cons and Scams 6) Cyberbullying	Pupils learn Acceptable use agreement fully, and poster in full also. Discussion of worst case scenarios. (see: Understanding the risks throughout e-safety policy) Pupils undertake 'Jigsaw' activity where pupil revise from last year: Full set of six wheels. where they are required to match the risks to the best and worst case scenarios, showing the different possible consequences of their choices. These wheels are to be displayed in the ICT suite afterwards. Emphasis made on the words 'risk' and 'choice' throughout. Challenge pupils to make a poster called either 1) "5 wrong clicks" and identify what their 5 things could be eg: a Parents credit card number. "Win £1,000,000 " ' or 2) "5 right clicks" eg: closing a chatroom conversation on an Xbox live game in which someone has asked for your email address. Pupils revise 4 ps sequence and flag to admin. Watch 'cuberbullying virus' video on youtube. Pupils learn 'What goes on the internet, stays on the internet.' And a 'selfie' can end up anywhere, out of our control. Understand emptional side of cyberbulling. Pupils learn how they can avoid being a cyberbully by making thought clouds to create empathy with victim and bully
6	To be aware of bias and misleading content on the internet. Uncompromising messages are to be sent such as 'There are videos on the internet of people being killed in car crashes, do you really want to see that?' Train younger children in e-safety	Learn acceptable use agreement fully. Expansion of Present posters as books, with a page explaining each point. Sexting warnings given and news articles from bbc shown, during Living and Growing PHSE theme. Pupils explore and research latest apps, evaluating their safety ina word document, At end of year, pupils undertake 'surviving and finding your place in the digital age. Where they discuss ethics and sensitivity in creating social networking etiquette, and also importance of having a relationship based on trust with parent. Pupils are given blank copies of all key word tables at end

		of year to remind them that they have the power to be savvy, know and recognize risks and make safe choices.

Theme 2 of 4 – Digital Cameras – term 1.

	Learning Outcomes	Suggested activities
R	To know that we must not take a picture of someone without asking first.	Role plays asking people politely before taking a picture of them.
1	To know that we should only take pictures of things our teacher has asked us to.	In all year groups, The part of the Keeping Salmestone e-safe poster is reiterated every time digital cameras are used: 1) We do not take images home on flash drives or memory cards. 2) We can only photograph the things and people our teachers tell us we can. (Teacher to check list in tray) 3) If anybody doesn't want to be photographed, we respect their decision.
2	To know that when we take a photograph of anyone, we must not save it to a computer and then pass it round to our friends.	
3	Staff and pupils are to ensure that pupils do not photograph peers for whom permission has not been obtained for them to be photographed in school and begin to take their own responsibility for this, for example on school trips.	
4	Pupils are to be taught that when taking digital photographs that they must never take the images off site in any way e.g.: on a flash drive or SD card.	
5	Advice should be given regarding background detail in a photograph which could identify the student or his/her location. (term 1)	
6	Pupils are taught that In the wrong hands digital photographs can be used for the wrong reasons.	Year 6 – sexting talk as part of living and growing. Illegal nature of acts made clear.

Theme 3 of 4 – Computer use at home term 3

	Learning Outcomes	Suggested activities
R		
1	To know the danger of giving out personal details on line.	Using http://www.thinkuknow.co.uk/5_7/leeandkim/default.aspx. Singing Superhero Sid's music video. Pupils make themselves an on-line character with a nickname e.g.: Crazyhair
2	To know how to stay safe in chat forums like club penguin. The greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links and occasionally access undesirable content.	Watching Lee and Kim's adventures and the HECTOR's world cartoons on http://www.thinkuknow.co.uk/5_7
3	Using e-mail and on line, pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc	Pupils are taught the 4 p's sequence for saving a troubling screen. 'press print screen, Open paint, paste and print during cyberbullying week. As it protects from cyberbullies as well as predators.
4	Pupils learn how to stay safe using technologies they themselves use.	Pupils use http://www.thinkuknow.co.uk/8_10/ to find out how to stay safe on line by choosing an activity they do on line at home and finding out how to do it safely.
5	Pupils are reminded of the E-SAFETY AUA and longevity of the internet. • Pupils learn that "**If you wouldn't**	Recap on http://www.thinkuknow.co.uk/8_10/ - star rider feature and cybercafe Use think u know website and the cybercafe to explore the

	be happy with it on display in a school corridor, don't write it anywhere on-line." As things can be later used against you. • Pupils should be encouraged not to use social networking sites till they reach the required age. However, the school recognizes that pupils will have access to them outside of school, and seeks to educate them as to the risks involved.	dangers of risk taking and then on school network to explore the themes further. Pupils role play a chat room conversation in which one person thinks they are talking to a friend but it in fact turns out to be an on-line predator. Pupils make an e-book of the school rules explaining the reasons behind each rule. In term 1 Pupils to watch the powerful and moving cyberbullying ceop video, then match it up with. Which rules were and were not followed. Notice, victim did NOT feel he had an adult he could trust. Mum DI print off and bring in evidence. Term 3 pupils play star rider
6	Pupils are given advice on the dangers of social networking. Pupils are shown print outs of facebook statuses that can make others feel down about themselves and taught to think of others and in on line behaviour Pupils are reminded that these are not to used by pupils of primary school age • Pupils should be advised not to place personal photos on any social network space till they are older. • They should consider how public the information is and consider using private areas. • Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. • Pupils should be encouraged to communicate with known friends only and deny access to others by making profiles private. • Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. They are to be • As with Staff, pupils are to consider that anything they say on-line could be made public/printed so they too should follow the principle of "**If you wouldn't be happy with it on display in a school corridor, don't post it anywhere on-line."** • As with Staff, pupils are to recognize that they are fully accountable for all their on-line activity and be aware of the power of the Police to identify and investigate the sender of inappropriate messages. • They shall learn what to do, if they believe they, or a friend of theirs is a victim of Cyber-Bullying via social networking: To let their parents or a member of staff know, who are to then inform the School leadership team.	Recap of the SMART rules from year 5. Q and A discussion on social networking with teachers. Teachers to explain why they feel safe on line at home and the steps they take to protect themselves.

Theme 4 of 4 – Cyberbullying – term 3

	Learning Outcomes	Suggested activities
R	X	X
1	X	X
2	X	X
3	1) Education as to what cyber bullying is, and the forms it can take. 2) Learning what can be done about it, who you should tell. 3) Being aware not only of your own vulnerability, but that of friends as well. 4) Pupils are to be made aware of the full extent of the seriousness of Cyberbullying – e.g.: exclusion from school and potential police involvement.	Discussion of all the ways someone could be unkind on line if they chose to. http://www.thinkuknow.co.uk/5_7/hectorsworld/ cartoon 6. Mindmap activity.
4	Pupils are to recognize that they are fully accountable for all their on-line activity and be aware of the power of the Police to identify and investigate the sender of inappropriate messages. Pupils must develop their understanding of what Cyberbullying is for three reasons: 1) So they can recognize it if they become a victim, and take appropriate action 2) So they can recognize it, if someone they know becomes a victim, and take appropriate action 3) Knowledge of the above should also make pupils aware of the serious nature of the distress caused by cyber bullying, the consequences involved and the fact that cyber bullying is not only immoral but illegal, thus the police can become involved.	Pupils design and make anti-cyberbullying posters with emphasis on what to do if you're being cyber bullied. PHSE drama about cyberbullying charting, cause, course and consequences.

5	• Pupils shall be taught that there are many examples of Cyber Bullying, including • 1 unkind/abusive messages via e-mail, facebook, text and instant messenger services such as msn or facebook chat. • 2 Creation of pages that are malicious or inappropriate. e.g.: forming a facebook group titled "We all hate Dave" directed against one individual or group. • 3 Directing peers or other on line friends to send unkind/abusive messages towards a person or group. • 4 making anonymous phone calls or sending anonymous text messages. • They shall learn what to do, if they believe they, or a friend of theirs is a victim of Cyber-Bullying: To let their parents or a member of staff know, who are to then inform the School leadership team. The leadership team will then investigate the matter immediately and thoroughly. For more information see section1.2.2 'What do I do if an e-safety issue comes to my attention?'	Pupils design and make anti-cyberbullying posters using school laptops and Microsoft publisher, with an emphasis on the ever expanding variety of forms it can take. Year 6 – exploration of the perils of trolling. Internet research about the consequences of this for victim and perpetrator.
6	Recap and pupil led expansion on the above.	Watch 'Cyberbullying' video from Think you know CD Rom.

6.1 Acceptable use Agreement for staff

Salmestone Primary School

Acceptable Use Agreement for ICT and e-safety - for Staff

- We commit to supporting the e-safety curriculum **and and upholding the** Keeping Salmestone e-safe **posters.**
- We use the 'What to do…' flow charts to guide actions in the event of an e-safety issue arising, including the 4 p's procedure of Print screen, open Paint, paste and print.
- We approach all e-safety matters with the ethos of asking ourselves: "Each time we use technology, what are the e-safety risks? What is the worst thing that could happen? How do we manage this risk?" as the following points are all written with this level of risk management in mind.

Internet use

- The only approved search engines for our school are, at present, www.ask.co.uk and www.kidrex.org
- For images we use the image search facility from www.ask.co.uk
- Staff are permitted to use google.com in the staff room, or whenever children are not present i.e: Out of teaching hours.
- Key stage one pupils are unlikely to be searching the internet independently. Should a teacher wish their pupils to do so, they must perform an on-line search beforehand and view the immediate results for age-suitability whilst assessing the websites.
- The school's WPA key is to remain confidential to staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.

E-mail

- Access must only be made via the authorized account and password which must not be made available to any other person, save members of the ICT team.
- Users are responsible for the e-mails that they send and contacts made.
- The same professional levels of language and content should be applied as for letters and media, particularly as e-mail is often forwarded.

Digital cameras

- Staff are to closely adhere to the lists of pupils who cannot be photographed and cannot be named, ensuring their faces are not photographed by adults or pupils
- Staff are responsible for ensuring pupils do not photograph peers for whom permission has not been obtained for them to be photographed in school.
- The publishing of pupils' names with their images without permission is dangerous and illegal, so not permitted unless written authorisation from their parent or guardian is obtained. This includes newspapers, the school website, or any other format.
- Staff are not to store photographs of children on a long term basis on USB flash drives or SD cards in case of theft or loss.
- Staff are to use the school's digital cameras as each class is provided with one. Taking photographs of children using members of staff's mobile phones is not permitted, for the protection of all involved.
- Staff are not to transfer images of children to their own hardware such as a mobile phone or home computer.
- Staff are to ensure that pupils do not remove images of themselves or others from school using portable media devices.
- Written permission from parents or carers will be obtained before images of pupils are taken, or named.

- Images of children can only be stored on teachers' laptops, the school's digital cameras and on the school's secure network.
- The school's Digital cameras are to be protected with a PIN or SWIPE pattern.
- Sometimes we are documenting children's work and need to take pictures of them and their progress. If parents have decreed that their pupil cannot be photographed then we need to respect this. Therefore I think the solution is that wherever possible, we only take pictures of these children's work. If it is unavoidable to avoid photographing the child (for example, when wishing to document climbing/balancing skills), then we must only take photos of these children from the neck down, or if their back is turned. If they are in a group then they would need to be hidden behind someone else. Their face cannot be visible. These pictures should then be deleted immediately after printing so that only the hard copy remains.
- Teachers are to shred any unused pictures of children.

Teachers' laptops

- Laptops are to be kept secure e.g. not to be left in a car overnight.
- Log-on information and passwords must be kept confidential between the user and the ICT Team alone.
- If a Supply teacher is required to log-in to a computer then a member of the ICT team is required to do this.
- Teachers must allow their computers to update windows and McAffee virus definitions.
- Laptops may be used for legitimate, everyday activity such as checking e-mail accounts and web surfing.
- Teachers' laptops are not to be used for inappropriate content.
- Staff are to be aware that Internet Explorer and Google Chrome record and remember all web addresses typed by the user.
- Staff are ultimately responsible for all activity that is undertaken on their laptop so must exercise caution over who uses it at home.

Data Protection

- When data is taken off site, great care must be taken to ensure that it is not lost, stolen copied or transferred. USB Flash Drives are particularly vulnerable due to their size. They are to be stored in a safe place at all times e.g., on a key ring, or in a laptop case. They should never be left in a car on display or overnight.
- Staff must never walk away from a laptop or computer they are logged onto and leave it unattended. This is because these computers now have access to our entire database of confidential pupil information. Use the windows key + L to lock your machine.
- Access to Servers must be located securely and are only to be accessed by qualified staff e.g. the ICT leader, ICT technician or Network manager.
- Data must be kept confidential to relevant and authorized parties. Discretion and responsible, professional conduct is essential.

Data protection act 1998

- Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.
- The following eight principles must be followed, to ensure compliance

Personal data must be:

1. _ Processed fairly and lawfully
2. _ Processed for specified purposes
3. _ Adequate, relevant and not excessive
4. _ Accurate and up-to-date
5. _ Held no longer than is necessary
6. _ Processed in line with individuals' rights
7. _ Kept secure
8. _ Transferred only to other countries with suitable security measures.

Other safety points in school

- Portable media e.g. USB Flash drives and SD cards that are brought in from home by staff or pupils may be used, provided all parties are certain that the existing content is thoroughly suitable for school. A virus check must be undertaken the moment it is plugged into a school computer.
- Videoconferencing is to be done via Flash meetings. Conferences should always be booked as private and not made public.
- Pupils and teachers will be taught to acknowledge the source of information used and to comply with copyright legislation.
- Staff are not to allow pupils access to their mobile phone e.g. to play a game on it during Golden Time.
- Iphones, Smartphones and other portable media that carry their own internet connection are not protected by KCN filtering, therefore it must be protected by a PIN or passcode, kept from pupils in a locker or zipped bag or kept on your person at school.
- Never plug in an unfamiliar or found flash drive without first getting it checked by the ICT team.
- If you believe you have encountered a virus, then the machine must be shut down, and not switched on again in school under any circumstances, as it could spread the virus across the school network. Please hand the machine to the ICT team at the first opportunity, who will then remove networking circuit boards before switching it on, to investigate the problem.

Using the Internet, Social Networking/Media, Instant messaging and e-mail at home safely

- All staff are to be aware of the potential risks of using social networking sites. To remain safe as a user of them, the following 9 principles need to be rigorously practiced.

1. All staff need to ensure their profiles are secured by using a website or e-mail facility's privacy settings to keep their profile private to the select audience of people they know. This minimizes the risk of personal information, private communications and photographs being disclosed to the media, or other public parties. It also provides protection against identity theft.
2. They should be aware of the importance of considering the material they post and how publishing unsuitable material may affect their professional status or the public image of our school. To be certain that staff are minimizing the risk of being compromised in this way, they should consistently apply the following principle to all on-line activity: "**If you wouldn't be happy with it on display in a school corridor, don't post it anywhere on-line."** This applies to photographs, autobiographical and personal information, published opinions, political and religious beliefs messages and status updates etc. This is to ensure that, should a parent or pupil somehow gain access to a member of staff's Facebook page, then the material they view will not compromise the teacher, with little likelihood of ramifications.
3. Whilst staff are encouraged to discuss political and educational issues in all suitable forums, staff are heavily advised to refrain from discussing school related matters and issues specific to our school on social networking sites or anywhere else on-line. Staff are to recognise that with any communications they make on-line, their words could be potentially printed and made public.
4. Malicious/inappropriate messages of any kind are particularly dangerous and may constitute cyberbullying. There have been several high profile cases in the media of staff writing unkind/malicious messages regarding a colleague which have resulted in disciplinary action being taken. Staff are to recognize that they are fully accountable for all their on-line activity and be aware of the power of the police to identify and investigate the sender of inappropriate messages.
5. Staff are never to communicate with students using social networking sites. If a pupil makes contact for example by email or by 'adding you as a friend' on Facebook, or any social networking/media service, then the teacher should either ignore the request, or send the following (fully permitted) message: "Thank you for your recent communication, however our schools e-safety policy means that staff can't be in contact with pupils or former pupils using Facebook or any social networking/media service. I wish you all the best. Signed: Mr/Miss/Mrs _____" They are not to have any further communication. This is part of staff general practice of keeping contact with pupils removed and separate from their personal lives and is primarily for the member of staff's own protection.
6. Staff are advised to look routinely look through all pictures of them that are on their social network pages or any other on-line forum they have subscribed to. The images should be checked rigorously for any signs of inappropriate content, imagining how things would look through the eyes of a parent or pupil. These should of course be hidden using our personal privacy settings, but a check is naturally wise as it can take surprisingly little for a picture to become public. For example; if a staff member's mobile phone with a Facebook page open, is somehow seen by a pupil.
7. Not all pictures of us are placed with our knowledge or consent, for example: pictures of a staff night out. Staff are advised to annually email/message everyone they know with a polite reminder that as we work with children, our profession requires that we are seen to have certain standards and can they please let us know before posting any picture of us on their network pages.
8. Staff should not place any pictures of other members of staff on their network pages without their permission.
9. No one should ever disclose their on-line or home computer passwords, inside or outside of school.

- For their own protection, staff should not allow any computer within school to 'remember' a private e-mail address.
- Staff are not to disclose private e-mail addresses e.g. Hotmail or Gmail. For any correspondence for matters concerning school, the approved TKAT 365 account is the only one that should be used
- Staff should not disclose even a school email account to pupils or parents as this places them in an inappropriate position where they could be potentially vulnerable to malicious allegations, unless via an approved transparent system such as a Virtual Learning Platform like Learnanywhere.

Youtube policy

As of September 2014, YouTube (https://www.youtube.com/) should become unlocked and de-firewalled, for use within lessons in school. This was a carefully considered decision on the part of our headteachers.

Whilst there are many schools that use YouTube safely, there are others who do not use it all and keep it firewalled. Therefore it is now important that we consider and manage the risks involved by carefully following the steps below. I will be adding all of these to our e-safety policy and acceptable use agreements, when they are up for their annual review.

- Firstly, there are many videos on YouTube which are thoroughly unsuitable, not only for school but for children in any situation. Videos such as those of a violent or sexual nature are present on YouTube, and must not be shown to children under any circumstances.
- Sometimes videos with this content can have seemingly innocent titles.
- You are entirely responsible for the YouTube videos you choose to show your class.
- YouTube videos should be viewed, in their entirety by the teacher, privately, before they are shown in class
- A search for YouTube clips should never be undertaken in front of children.
- When YouTube video is loaded up, there are many recommended similar videos that appear too. These are random videos that you, the user, have no control over. Therefore the following method is to be used for showing YouTube videos.
- The monitor is to be blanked or frozen, and the laptop turned away from children.
- The video is to be loaded into a web browser, paused immediately, then the video maximised to full screen resolution. This hides all other recommended videos.
- The projector can now show the laptop display freely, and the video can be played.
- The video should be paused moments a few seconds before the end, as this will prevent the display of another set of recommended videos.
- The screen can then be blanked or frozen, whilst the YouTube window is closed.
- Pupils are never to access https://www.youtube.com/ in school personally .
- The ICT leader is available to demonstrate this procedure.

Salmestone Primary School

Acceptable Use Agreement for ICT and e-safety - for Staff

Return slip

The above agreement represents a commitment to upholding the highest standards in e-safety

I agree to the terms specified above and recognize their importance in managing e-safety risks, and in safeguarding ourselves and the pupils in our care.

Name: _____

Signed : _____

Date : _____

Signature from ICT leader/ E-safety officer:

_____

Please submit this form to the school office.

Permission is thus granted to use the ICT facilities at Salmestone Primary School. We hope you enjoy using our ICT facilities.

6.2 Acceptable Use Agreement for pupils

Salmestone community primary school

Acceptable Use Agreement for ICT and e-safety - for Pupils and Parents

Using Computers and the internet

- I know why I need to follow the '*Keeping Salmestone e-safe*' posters.
- I know why I must never give away personal details online.
- I know why we only use safe search engines such as: www.ask.co.uk www.kidrex.org.
- I know I can click on HECTOR PROTECTOR the dolphin if I see something I don't like.
- I know I can only use the internet when there is an adult there to check I am safe.
- I know why I must never deliberately search for rude or nasty things.
- I understand that the school might check through my computer files and may check the sites I visit.
- I know that if I am irresponsible in my internet use, then I may be banned from using any computers at school.
- I know why I must not arrange to meet anybody who I have only met on the computer.

E-mail, V.L.E. and other internet subscriptions

- I only use accounts that our school has approved such as the VLE, Espresso, Education City or Activelearn.
- I do my best to remember my login numbers and passwords.
- I only ever use my own account, keeping my password secret and I don't touch other peoples work.
- I only e-mail or message people I already know in the real world.
- The messages I send will be polite, kind and sensible.
- I know I can immediately tell a teacher, or Mr Arnold if I receive a message that is unkind or upsetting. This includes incidents on Facebook, and X-box live.
- I know I can hit the 'Flag to Admin' button, if I receive a VLE message that I don't like.
- I know that I can bring in evidence such as print outs, to help adults understand things.

Digital Cameras, Mobile Phones and other areas of ICT

- I will check with teachers before taking any digital photographs.
- When using a camera on a school trip, I will firstly check who I can take pictures of.
- If I bring in a USB Flash drive or SD card, I know why I must check that everything on it is totally suitable for school. As soon as I get into school, I will give it to my teacher straight away so that they can run a virus check on it and keep it safe.
- I know why I must not save pictures taken at school, and then take them home on a USB flash drive or SD card.
- I will not touch my teacher's mobile phone.
- I will not copy work from the internet and pretend that it is mine.
- If I bring my mobile phone into school, I hand it in to my teacher for safe keeping, unless I need it to show a teacher about something nasty that has happened.

RETURN SLIP FOR: E-safety Acceptable use agreement

- Permission can only be granted to use the internet, and all other ICT facilities at Salmestone Primary School upon the return of this slip. We look forward to receiving it and hope you enjoy learning using our ICT facilities.

NAME: _____ **CLASS:** _____ **Date:** _____

Signature of pupil: _____

Signature of parent: _____

- ***7.1 Keeping Salmestone e-safe poster for KS1***

Supplied by KCC and EIS as of Easter 2014

- ***7.2 Keeping Salmestone e-safe poster for KS2***