e-Safety Policy

Version 1:0

Date Released: September 2019

Date to be reviewed: September 2020

Approved by: **Date:**

Why does a School need an e-Safety Policy?

- In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

- E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

- The Sallygate School must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating pupils and staff about responsible use. We must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

- Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

- Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and with Channels and Choices.

- The e-Safety policy is essential in setting out how the school plans to develop and establish its e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

- This e-Safety Policy is part of many different schools policies including the, Child Protection or Safeguarding Policies, Anti-Bullying Policy and the School Improvement Plan and relates to other policies including those for behaviour, for personal, social and health education (PSHE) and for citizenship.

- The Sallygate School has appointed an e-Safety Coordinator to lead on e-Safety. The person who is appointed does not need to have vast technical knowledge; however it would be helpful if they had some basic understanding of ICT.

- The school's Designated Safeguarding Lead (DSL) will also need to be aware of e-Safety training and resources and be available should any child wish to disclose information regarding an online incident. The DSL must be made aware of any disclosures, incidents or Child Protection concerns. The Senior Leadership Team and Channels and Choices are involved and will review the e-Safety policy annually and monitor its impact. They will also need to ensure that they take responsibility for revising the e-Safety policy and practice where necessary (such as after an incident or change in national legislation).

- The Headteacher and Channels and Choices have a legal responsibility to safeguard children and staff and this includes online activity.

- The e-Safety Policy and its implementation will be reviewed annually.

- Our e-Safety Policy has been written by the school, building on the KCC e-Safety Policy and government guidance.

- Our School Policy has been agreed by the Senior Leadership Team and approved by Channels and Choices.

Teaching and learning

Why is Internet use important?

Discussion:

- The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday 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.

- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

- 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 functions.

- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

How does Internet use benefit education?

Discussion:

- A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

- Benefits of using the Internet in education include:
  - access to worldwide educational resources including museums and art galleries;
  - educational and cultural exchanges between pupils worldwide;
  - vocational, social and leisure use in libraries, clubs and at home;
  - access to experts in many fields for pupils and staff;
  - professional development for staff through access to national developments, educational materials and effective curriculum practice;
  - collaboration across networks of schools, support services and professional associations;
  - improved access to technical support including remote management of networks and automatic system updates;
  - exchange of curriculum and administration data with KCC and DfE;
  - access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Developing effective practice in using the Internet for teaching and learning is essential.

Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material will be taught. Methods to detect plagiarism will need to be developed.

- The school's Internet access will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- 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 taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

- The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach will be required.

- Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc. provide an opportunity for pupils to develop skills in evaluating Internet content. For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils will use age-appropriate tools to research Internet content.

- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained?

- It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

- ICT security is a complex issue which cannot be dealt with adequately within this document. A number of agencies can advise on security including EiS and network suppliers.

  - The EIS IT Security Document Library: www.eiskent.co.uk?itsecurity

  - Local Area Network (LAN) security issues include:

  - Users must act reasonably -e.g. the downloading of large files during the working day will affect the service that others receive.

  - Users must take responsibility for their network use.

  - Workstations should be secured against user mistakes and deliberate actions.

  - Servers must be located securely and physical access restricted.

  - The server operating system must be secured and kept up to date.

  - Virus protection for the whole network must be installed and current.

- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

- Wide Area Network (WAN) security issues include:

  - Central KPSN Schools Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools.

  - Decisions on WAN security are made on a partnership between schools and KCC/EiS.

- The Schools Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes in Maidstone and Canterbury. These industry leading appliances are monitored and maintained by a specialist security command centre.

- The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly.

  - Personal data sent over the Internet or taken off site will be encrypted.

  - Portable media may not be used without specific permission followed by an anti-virus / malware scan.

- Unapproved software will not be allowed in work areas or attached to email.

  - Files held on the school's network will be regularly checked.

  - The ICT coordinator / network manager will review system capacity regularly.

  - The use of user logins and passwords to access the school network will be enforced.

<u>How will email be managed?</u>

- Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created, for example.

- The implications of email use for the school and pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

- A central question is the degree of responsibility that can be delegated to individual pupils as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible. In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- The use of email identities such as john.smith@school.kent.sch.uk needs to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people. Email accounts should not be provided which can be used to identify both a pupil's full name and their school. The Sallygate School will limit pupils to email accounts approved and managed by the school. For primary schools, whole-class or project email addresses should be used. When using external providers to provide pupils with email systems, schools must pay close attention to the sites terms and conditions as some providers have restrictions of use and age limits for their services.

- Spam, phishing and virus attachments can make email dangerous. The Kent Public Service Network uses industry leading email relays to stop unsuitable mail using reputation filtering. Currently about 95% of email is rejected as spurious.

Possible statements:

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed?

- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)

- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

- Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

- Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" will replace "passport style" photographs but still convey the educational activity. Pupils in photographs should, of course, be appropriately clothed.

- Images of a pupil will not be published without the written permission of the parent / those holding parental authority. The Sallygate School will ask permission to publish images of work or appropriate personal photographs on entry, and again annually.

- Pupils also need to be taught the reasons for caution in publishing personal information and images online (see previous).

- Please see the Children's Safeguards site, "Use of photographic images of children" www.kenttrustweb.org,uk?safeguards (Policy and Guidance section) for guidance on Photographic Policies.

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

    - Pupils work can only be published with their permission or the parents/those with parental authority.

    - Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

How will social networking, social media and personal publishing be managed?

- Parents/those with parental authority and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

- For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

- The use of social networking sites in school or using school equipment is not permitted at The Sallygate School..

- Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- Additional guidance and considerations for schools around this topic (including a checklist and risk assessment templates) can be found in the "Using Social Media and Technology in Educational Settings" document at www.kenttrustweb.org.uk?esafety

- Schools may wish to consider creating a separate social media policy to outline actions taken to reduce risk and to highlight the benefits of using social media.

- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers/those with parental authority, particularly when concerning pupils' underage use of sites.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff.

How will filtering be managed?

- Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles must be appropriate for all members of the school community. Older secondary pupils, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

- Access controls fall into several overlapping types (commonly described as filtering):

    - Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.

    - A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of content.

    - Dynamic content filtering examines web page content or email for unsuitable words.

    - Keyword lists filter search engine searches and URLs for inappropriate results and web addresses. Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.

  - URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.

  - Key loggers record all text sent by a workstation and analyse it for patterns.

- Schools installing or managing their own filtering systems and policies must be aware of the responsibility and demand on management time. Thousands of inappropriate sites are created each day and many change URLs to confuse filtering systems. It is the Senior Leadership Team's responsibility to ensure appropriate procedures are in place and all members of staff are suitably trained to supervise Internet access.

- It is important that schools recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone).

- Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that Acceptable Use Policies are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online. There will also be an Incident Log to report breaches of filtering or inappropriate content being accessed. Procedures need to be established to report such incidents to parents/those with parental authority and KCC (The Schools Broadband Service Desk at EiS or the e-Safety Officer) where appropriate.

- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF, Kent Police or CEOP (see e-Safety contacts and references).

- Websites which schools believe should be blocked centrally should be reported to the Schools Broadband Service Desk. Teachers should always evaluate any websites/ search engines before using them with their pupils; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.

- The school will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed.

- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.

- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

  - The School filtering system will block all sites on the Internet Watch Foundation

(IWF) list.

- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.

- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP

- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

How are emerging technologies managed?

- Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access: collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed.

- Access will be denied until a risk assessment has been completed and safety has been established.

- Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

- The safety and effectiveness of virtual communities depends on users being trusted and identifiable. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

- New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher’s reaction in a difficult situation.

- Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many pupils and families; this could be used to communicate a pupil's absence or send reminders for exam coursework. Staff must not use personal phones to contact pupils.

- The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy.

- Abusive messages should be dealt with under the school's behaviour and/or anti-bullying policies.

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

- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school during PHSE lessons. Pupils may not bring mobile phones to school.

How should personal data be protected?

- The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

- The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

- Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

- The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

  - Processed fairly and lawfully
  - Processed for specified purposes
  - Adequate, relevant and not excessive
  - Accurate and up-to-date
  - Held no longer than is necessary
  - Processed in line with individual's rights
  - Kept secure
  - Transferred only to other countries with suitable security measures

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

Policy Decisions

How will Internet access be authorised?

- The school will allocate Internet access to staff and pupils on the basis of educational need. It should be clear who has Internet access and who has not. At The Sallygate School authorisation is generally on an individual basis.

- Normally most pupils will be granted Internet access; it may be easier to manage lists of those who are denied access. Parental permission/permission from those with parental authority will be obtained for Internet access in all cases as new pupils join, and this will be held on the pupil file. Pupils will not be prevented from accessing the internet unless the parents/those with parental authority have specifically denied permission or the child is subject to a sanction as part of the school behaviour policy.

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

    - All staff will read and sign the 'Staff Information Systems Code of Conduct' or School Acceptable Use Policy before using any school ICT resources.

    - Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

    - All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.

    - Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

    - When considering access for vulnerable members of the school community, the school will make decisions based on the specific needs and understanding of the pupil(s).

- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

- Secondary pupils will apply for Internet access individually by agreeing to comply with the School e-Safety Rules or Acceptable Use Policy.

How will risks be assessed?

- As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation.

- The school will take 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 Channels and Choices can accept liability for the material accessed, or any consequences resulting from Internet use.

- The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of 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 and breaches will be reported to Kent Police.

- Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

- Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used. This e-Safety Policy recognises and seeks to develop the skills that children and young people need when communicating and using technologies enabling them to keep safe and secure and act with respect for others.

- e-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

- Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Child Protection Coordinator.

- The Sallygate School will utilise the template provided by Kent County Council to manage incidents: "Response to an Incident of Concern": http://www.kenttrustweb.org.uk?esafety

- Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, The Sallygate School will determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting the Children Safeguard Team or

- Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

- Possible statements:

  - All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

  - The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.

  - The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

- The school wifi manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other school in Kent.

How will e-Safety complaints be handled?

- Parents/those with parental authority, teachers and pupils should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. e-Safety incidents may have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.
- A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which will be linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or e- Safety Coordinator, Advice on dealing with illegal use can, when deemed necessary, be discussed with the Kent Police Safer Schools Partnership Coordinator responsible for the school or the Children's Safeguard Team.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e-Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents/stakeholders will be informed of the complaints procedure. Parents/stakeholders and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of

confidentiality and the need to follow the official school procedures for reporting concerns.

- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community?

- Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, and supermarket or cyber cafe. Ideally, young people would encounter a consistent internet use policy wherever they are.
- Regarding internet access in the community, there is a fine balance between ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Organisations are developing access appropriate to their own client groups and pupils may find variations in the rules and even unrestricted Internet access. Although policies and practice may differ, community partners adhere to the same laws as schools. As part of school development, staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with pupils on the reasons for the differences could be worthwhile.
- Sensitive handling of cultural aspects is important. For instance filtering software should work across community languages and school Internet policies may need to reflect the pupils' cultural backgrounds. Assistance from the community in drawing up the policy could be helpful.
    - The school will liaise with local organisations to establish a common approach to e- Safety.
    - The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
    - The school will provide appropriate levels of supervision for pupils who use the internet and technology whilst on the school site.

How will Cyberbullying be managed?

- Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

- Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

- It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

- There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:
    - Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils.
    - These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents.
    - Gives head teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

- Where bullying outside school (such as online or via text) is reported to The Sallygate School, it will be investigated and acted on.

- Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police.

- For more information please read "Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies" http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying

- DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying http://www.digizen.org/cyberbullying

- Possible Statements:

    - Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti- bullying and behaviour.

    - There are clear procedures in place to support anyone in the school community affected by cyberbullying.

    - All incidents of cyberbullying reported to the school will be recorded.

    - There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

        - Pupils, staff and parents//those with parental authority, carers will be advised to keep a record of the bullying as evidence.

        - The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

- Sanctions for those involved in cyberbullying may include:

    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.

    - Parent/carers of pupils will be informed.

    - The Police will be contacted if a criminal offence is suspected.

<u>How will mobile phones and personal devices be managed?</u>

- Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features. However, pupils are not permitted to bring to, or to use such devices at The Sallygate School because mobile phones can present a number of problems when not used appropriately:

    - They are valuable items which may be stolen or damaged;

    - Their use can render pupils or staff subject to cyberbullying;

    - Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.

    - They can undermine classroom discipline as they can be used on "silent" mode;

- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

- Staff are given clear boundaries on professional use.

Pupils Use of Personal Devices

- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

- Staff will be issued with a school phone where contact with pupils or parents/carers is required.

- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

How will the policy be introduced to pupils?

- Many pupils are very familiar with culture of mobile and Internet use. As pupils' perceptions of the risks will vary; the e-Safety rules may need to be explained or discussed.

- Consideration will be given as to the curriculum place for teaching e-Safety. This could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever pupils are using the internet.

- Useful e-Safety programmes include:

    - Think u Know: www.thinkuknow.co.uk

    - Childnet: www.childnet.com

    - Kidsmart: www.kidsmart.org.uk

  - Orange Education: www.orange.eo.uk/education
  - Safe: www.safesocianetworking.org

- All users will be informed that network and Internet use will be monitored.

- An e-Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils. Pupil instruction regarding responsible and safe use will precede Internet access.

- An e-Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.

- e-Safety rules or copies of the pupil Acceptable Use Policy will be posted in all rooms with Internet access.

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- It is important that all staff feel confident to use new technologies in teaching and the School e-Safety Policy will only be effective if all staff subscribe to its values and methods.

- Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

- All staff must understand that the rules for information systems misuse for employees are specific and that contravention of these rules may result in disciplinary procedures. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

- Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. The Sallygate School is clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff are made aware of their responsibility to maintain confidentiality of school information.

- Induction of new staff should include a discussion about the school e-Safety Policy.

- The e-Safety Policy will be formally provided to and discussed with all members of staff. To protect all staff and pupils, the school will implement Acceptable Use Policies.

- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will the support of parents/those with parental authority be enlisted?

- The use of the internet is strictly controlled in Channels and Choices homes.
- Attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- Parents/placing authorities will be requested to sign an e-Safety / Internet Agreement as part of the Home School Agreement.
- Stakeholders will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Interested stakeholders will be referred to organisations listed in the "e-Safety Contacts and References section".

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.poljce.uk

e-Safety Officer, Children's Safeguards Team, Families and Social Care, Kent County Council. The e-Safety Officer is Rebecca Avery email: esafetyofficer@kent.gov.uk
Tel: 01622 221469
Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Officer for Training & Development, Children's Safeguards Team, Families and Social Care, Kent County Council:

The Children's Officer for Training & Development is Mike O'Connell Tel: 01622 696677; email: mike.oconnell@kent.gov.uk

Children's Safeguards Team: www.kenttrustweb.org,uk?safeguards

Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.ejskent.co,uk

Internet Watch Foundation (IWF): www.jwf.org.uk

Kent e-Safety in Schools Guidance: www.kenttrustweb.org.uk?esafety

Kent Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 01622 690690 or contact your Safer Schools Partnership Officer.

Also visit www.kent.police.uk or www.kent.poljce.uk/internetsafety

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kidsmart: www.kidsmart.org.uk

Schools Broadband Service Desk - Help with filtering and network security: www.eiskent.co.uk Tel: 01622 206040

Schools e-Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think u Know website: www.thinkuknow.co.uk

Virtual Global Taskforce - Report Abuse: www.virtualglobaltaskforce.com

Schools e-Safety Audit

This self-audit has been completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff contributing to the audit include: **Designated Safeguarding Lead(s), e-Safety Coordinator, Class Teachers**

Has the school an e-Safety Policy that complies with Kent guidance?	
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by Channels and Choices on:	
The policy is available for staff to access at:	
The policy is available for stakeholders to access on request to the school.	
The responsible member of the Senior Leadership Team is:	
The Designated Safeguarding Lead is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?	
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	
Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the schools expectation around safe and professional online behaviour?	
Is there a clear procedure for staff, pupils and parents/carers to follow when responding to or reporting an e-Safety incident of concern?	
Have e-safety materials from been distributed to pupils?	
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	
Has an ICT security audit been initiated by SLT?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	

Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	
Does the school log and record all e-Safety incidents, including any action taken? (Debriefing Notes)	
Are Channels and Choices and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	