Lanesend Primary School

E-Safety Policy

Statutory Policy

Signed: …… Date:
(Headteacher)

Signed: …… Date:
(Chair of Governors)

Review Date: March 2020 (Every 2 Years)
Reviewed By: Computing Manager and Child-Centred Group

Lanesend Primary
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' that applies to everyone working with children.

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating children and staff about responsible use. Schools 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.

Families have a responsibility to ensure they uphold robust e-Safety practices at home and monitor their children's online activities. Children should be as protected at home as they are in a school setting.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, children 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 Headteacher and the Governing body.

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.

Reviewing the policy

The E-Safety Policy is part of many different schools policies including the Curriculum Policy, Child Protection or Safeguarding Policy and Anti-Bullying Policy and should relate to other policies including those for behaviour, for personal, social and health education (PSHE) and for citizenship. Policy construction provides a method to review practice - in this case the use of technology and its benefits and risks. The more that staff, families, governors and children are involved in deciding and creating the policy, the more effective it will be.

It is recommended as best practice that all schools appoint 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 Computing.

The school's Designated Child Protection Coordinator (DCPC) will need to be aware of e-Safety training and resources and be available should any child wish to disclose information regarding an online incident. Therefore it may be an idea to elect them as e-Safety representative. However another member of staff may be selected. The DCPC must be made aware of any disclosures, incidents or Child Protection concerns. The Progression Team and Governing Body must be involved and should 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 governing body have a legal responsibility to safeguard children and staff and this includes online activity.

- The school has appointed an e–Safety Coordinator.
- The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on government guidance.
- Our School Policy has been agreed by the Child Centered Group and approved by governors and other stakeholders.
- The School has appointed a member of the Governing Body to take lead IN Safeguarding, which includes E-Safety.

The School e-Safety Manager is **Graham Andre**

The e-Safety IT Management is **IIF.**

Teaching and learning

Using the Internet

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 Computing 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 children with safe quality Internet access as part of their learning experience, working in partnership with families
- Children 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, e.g. social networking sites such as Facebook
- 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 children who show a responsible and mature approach to its use (see Acceptable Use Agreement).
- School has a duty to provide an e-Safety curriculum

Use of World Wide Web in the Classroom

There are two agreed procedures for the use of video and streaming in the classroom.

1. If staff have preplanned to show a video, they must either paste the link into a PowerPoint or use Safeshare - https://safeshare.tv/
2. If staff are using the Internet, including YouTube, spontaneously they must turn off the TV to check suitability first and must stay at the computer to start and stop videos. Autoplay must be turned off.

- Vimeo is not to be used and will remain blocked.
- Staff are to check that streaming sites are used safely and content is appropriate for the children before use in the classroom.
- In all instances, staff members must be by a computer ready to start and stop videos when they are being used.
- This applies to all staff, including Squirrel's Den staff, both during term time and in the holidays.

Benefits

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

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between children worldwide (e.g. Skype);
- vocational, social and leisure use in libraries, clubs and at home;

- access to experts in many fields for children 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 the DfE;
- access to learning wherever and whenever convenient.

Enhancing Learning

Increased computer numbers and improved Internet access may be provided but its impact on children's learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Children 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 should be taught. Methods to detect plagiarism may need to be developed.

- The school's Internet access will be designed to enhance and extend education.
- Children 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 children complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of children.
- Staff should guide children to online activities that will support the learning outcomes planned for the children' age and ability. However, independent learners may come across inappropriate material.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. "fake news");
- Children will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

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

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

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

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 children.

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.
- 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 and password controlled.

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 Lanesend Primary and IFF.

The Schools Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes managed by Wight Fibre. 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 i.e. Ipads 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 manager and network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

Managing email

Email is an essential means of communication for both staff and children. 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 children need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to children that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual children 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.

- Children may only use approved email accounts for school purposes.
- Children must immediately tell a designated member of staff if they receive offensive email. This applies to both mail sent in and outside of school.
- Children 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 children and families, as approved by the Progression 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.
- Staff should not use personal email accounts during school hours or for professional purposes.

Publishing on the internet

Many schools have created excellent websites and communication channels, which inspire children to publish work of a high standard. Websites can celebrate children's work, promote the school and publish resources for projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

Sensitive information about schools and children could be found in a newsletter but a school's website is more widely available. Publication of any information online should always be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.

- The contact details on the website should be the school address, email of individual staff members and telephone number. Staff or children's personal information must not be published.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- The Headteacher will take overall editorial responsibility for online content published by the school, including school class blogs, and will ensure that the 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.

Publishing children images and work

Still and moving images and sound add liveliness and interest to a publication, particularly when children can be included. Nevertheless the security of staff and children is paramount. Please see our Use of Images Policy for further information.

Managing social networking, social media and personal publishing

Families 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. Children 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.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with children or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

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.

A checklist and risk assessment templates can be found at the end of this document.

Social Media

- The school will control access to social media and social networking sites including ‘Class Dojo’. Mobile phones can be left in the office at the beginning of the day and collected at the end. Mobile phones for children will not be allowed in school. Mobile phones for staff will be for personal use and only during rest times.
- Children will be advised never to give out personal details of any kind that 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.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Headteacher. Members of staff are advised not to run social network spaces for children’s use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

- Children will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Children will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- Children will be educated on how to stay safe on social networking sites. These sites are filtered on the school computers.

- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding children' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their families, particularly when concerning children' underage use of sites and this will be reported to the Social Media provider.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.
- Staff are not to be 'friends' on social networking sites with children and, where possible, families.

Managing inappropriate material

Levels of Internet access and supervision will vary according to the children's age and experience. Access profiles must be appropriate for all members of the school community.

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. This is managed by IIF.
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit children's 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.

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.

In addition, Internet Safety Rules should be displayed, and both children and adults are educated about the risks online. There is also an Incident Log to report breaches of filtering or inappropriate content to the Headteacher, Computing Lead and IIF.

Any material that the school believes is illegal must be reported to appropriate agencies.

Teachers should always evaluate any websites/search engines before using them with their children; this includes websites shown in class as well as websites accessed directly by the children. Often this will mean checking the websites, search results etc 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 children.
- The school will work with the Computing Lead to ensure that the 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 children) will be aware of this procedure.
- If staff or children 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 sites and be managed by IFF.
- 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 Progression Team and Computing Lead.
- The School Development Manager in conjunction with IIF 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 the police.
- It is vitally important any incidents are recorded.

Managing video conferencing

Video conferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education.
Equipment ranges from small PC systems (web cameras) to IPad and video recorders.

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Video conferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School video conferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the video conferencing equipment outside school time will be established with care.

Users

- Only teachers will make or answer a video conference call.
- Video conferencing will be supervised appropriately for the children's age and ability.
- Families consent should be obtained prior to children taking part in video conferences.
- Unique log on and password details for the educational video conferencing services should only be issued to members of staff and kept secure.

Content

- When recording a video conference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of video conference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a video conference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

Managing emerging technologies

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. The safest approach is to deny access 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. This may not be easy, as authentication beyond the school may be

difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

The inclusion of inappropriate language or images is difficult for staff to detect. Children 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 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.
- Children will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

Personal data protection and GDPR

The quantity and variety of data held on children, 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. This must be communicated to the individual. 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.

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.

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

Internet access will be authorised

The school should allocate Internet access to staff and children on the basis of educational need. It should be clear who has Internet access and who has not. At Lanesend pupil usage will be fully supervised. All children in a class could be authorised as a group.

Parental permission is safest for Internet access in all cases. Children are not prevented from accessing the internet, unless the families have specifically denied permission or the child is subject to a sanction as part of the school behaviour policy. We will record all children who are denied access. Permission forms will be sent out to families, when starting school in Reception.

- The school will maintain a current record of all staff and children who are granted access to the school's electronic communications.
- Families will be asked to read the Acceptable Use Policy for children's 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.
- Families will be informed that children will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) we will make decisions based on the specific needs and understanding of the child.

- At Early Years Foundation Stage and Key Stage 1, children's access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2, children will be supervised. Children will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

Assessing risks

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. We will need to address the fact that it is not possible to completely remove the risk that children might access unsuitable materials via the school system.

Risks can be considerably greater where tools are used which are beyond the schools control such as most the popular social media sites i.e. Facebook.

- 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. The school cannot 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 Hampshire (IW) Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Responding to incidents of concern

Staff will 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, Caroline Sice.

Staff will use the template provided by Lanesend Primary to manage incidents: "Response to an Incident of Concern"

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, schools should 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 and the LADO, if the offence is deemed to be out of the remit of the school to deal with.

- 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 will manage e-Safety incidents in accordance with the behaviour policy where appropriate.
- The school will inform families of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, indentify 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 LADO and escalate the concern to the Police**.**

- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer (Hampshire) to communicate to other schools on the Isle of Wight.

Handling e–Safety complaints

Families, teachers and children 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 children, 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 the Headteacher. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator and e–Safety Coordinator. Advice on dealing with illegal use can, when deemed necessary, be discussed with the LADO and Hampshire 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 Headteacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Children and families will be informed of the complaints procedure.
- Families and children 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 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.

Internet use across the community

- The school will liaise with local organisations, cluster schools and secondary schools to establish a common approach to e–Safety.
- The school will be sensitive to Internet-related issues experienced by children out of school, e.g. social networking sites, and offer appropriate advice.

- The school will provide appropriate levels of supervision for children who use the internet and technology whilst on the school site.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on site.

Managing cyber bullying

Cyber bullying 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 families 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 that 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 children. These measures are part of the school’s behaviour policy which is communicated to all children, school staff and families
- gives headteachers the ability to ensure that children 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 school, it should 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.

- Children will be taught the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

- Cyber bullying (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.
- Children, staff and families 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.
- Children, staff and families 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 children and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Families of children will be informed.
- The Police will be contacted if a criminal offence is suspected.
- The Local Authority legal department will be contacted to help manage cyber bullying.

Managing mobile phones

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, 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 children or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow children 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 children or staff.

At Lanesend, we prohibit children from taking mobile phones into the classroom. Mobile phones can be left at the school office and collected at the end of the day so that families can ensure health and safety to and from school.

- The use of mobile phones and other personal devices by children and staff in school will be decided by the school and covered in the school Mobile Phone Policy.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Headteacher with the consent of the child or families. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time. They will be left at the school office.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in school or when visiting other establishments (on school trips/visits).

Children's Use of Personal Devices

- If a child breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to families in accordance with the school policy.
- Phones and devices must not be taken into examinations. Children found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the child's withdrawal from either that examination or all examinations.
- If a child needs to contact their families they will be allowed to use a school phone. Families are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Children should protect their phone numbers by only giving them to trusted friends and family members. Children will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

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 or have permission to use their personal phones to make contact with the school or families if 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 to the Headteacher in emergency circumstances.
- If staff use personal devices such as mobile phones or cameras to take photos or videos of children then the photos or videos are saved to the school file and deleted from the phone.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication

Lanesend Primary encourages regular visits from the local police.

- 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 children.
- Instruction to children regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or Computing programs covering both safe school and home use.
- e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- e-Safety rules will be posted in the ICT room.
- 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 children are considered to be vulnerable – to include Looked After Children, Child Protection, CAF families

Staff communication

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 should 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 instances resulting in disciplinary procedures and dismissal have occurred. 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 that may be accessed outside of the school network. Schools must be 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 must be made aware of their responsibility to maintain confidentiality of school information.

ICT use is widespread and all staff including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. 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 children, the school will implement an Acceptable Use Policy.
- 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 Headteacher and have clear procedures for reporting issues.
- The School will highlight useful online tools that staff should use with children in the classroom. These tools will vary according to the age and ability of the children.
- 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.

Supporting safe e-safety at home

Internet use in children' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless families are aware of the dangers, children may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help families plan appropriate, supervised use of the Internet at home and educate them about the risks. Families should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy.

We will help families to understand more about ICT by running courses and parent awareness sessions.

Lanesend Primary is committed to providing in-school e-Safety sessions with the local police, for families.

- Families' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with families will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Families will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Families will be encouraged to read the school Acceptable Use Policy for children and discuss its implications with their children.
- Information and guidance for families on e–Safety will be made available to families in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to families.

Lanesend Primary e-Safety Audit

This self-audit should be completed by the member of the Progression Team responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Headteacher.

Has the school an e-Safety Policy that complies with Local Authority guidance?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for families to access at:	
The responsible member of the Progression Team is:	
The governor responsible for Safeguarding is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. children, staff and families) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N
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?	Y/N
Is there a clear procedure for staff, children and families to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y/N
Is e-Safety training provided for all children (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in the ICT Room?	Y/N
Do families and children sign an Acceptable Use Policy?	Y/N
Are staff, children, families and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by the Progression Team?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act and GDPR?	Y/N
Is Internet access provided by an approved educational Internet service provider that complies with DfE requirements (e.g. KPSN)?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by the Headteacher?	Y/N

Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by the Headteacher?	Y/N
Does the school log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and Progression Team monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	Y/N

e-Safety Contacts and References

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

e–Safety Officer

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Officer for Training & Development,

Children's Safeguards Team:

Click 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:

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

www3.hants.gov.uk/childrens-services/schoolsandcolleges/esafety

Hampshire and Isle of Wight Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Hampshire & IoW Police via 0845 045 4545 or contact your Safer Schools Partnership Officer.
Also visit www.hampshire.police.uk or
www.hampshire.police.uk/internet/advice-and-information/general/online-safety

Isle of Wight Safeguarding Children Board (4LSCB) www.4lscb.org.uk/isleofwight

Kidsmart: www.kidsmart.org.uk

Schools Broadband Service Desk - Help with filtering and network security:

Schools e–Safety Blog:
www.nfer.ac.uk/emie/inc/fd.asp?user...4LSCB**ESafety**Strategy(1).pdf

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

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

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