****

**Lenham Primary School**

**Online Safety Policy,**

**Including Acceptable Use Policy**

**October 2016**

****

**Aims**

Lenham Primary School believes that online safety (E-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

We identify that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online. We respect our role in protecting staff and children from potential harm.

The school has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

**Purpose**

The purpose of this E-Safety policy is to:

* + Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Lenham Primary School is a safe and secure environment.
	+ Safeguard and protect members of our community online.
	+ Raise awareness with all members of our community regarding the potential risks as well as benefits of technology.
	+ To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
	+ Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as ‘staff‘ in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) ‘Safeguarding and Child Protection’, ‘Anti-Bullying’ and ‘Behaviour and Discipline’.

**The Designated Safeguarding Lead (DSL) is: Anji Martin**

**The Online safety (e-Safety) lead for the Governing Body is: Ceri Norey**

**Policy approved by Head Teacher: Sarah Howell Date: 15/10/16**

**The date for the next policy review is: November 2017**

*It is advisable for this policy to be reviewed at least annually*

The policy has been written by the school, involving staff, pupils and parents/carers, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.

**Key responsibilities for the community**

The key responsibilities of the school’s leadership team (SLT) are:

* Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
* Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
* Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
* Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an ‘Acceptable Use Policy’ which covers appropriate professional conduct and use of technology.
* To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
* To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.
* Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
* Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
* To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
* Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
* Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
* Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
* To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety: Ceri Norey
* Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

The key responsibilities of the Designated Safeguarding Lead are:

* Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
* Keeping up-to-date with current research, legislation and trends regarding online safety.
* Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
* Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
* Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
* Monitor the school’s online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need
* To report to the SLT, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
* Liaising with the local authority and other local and national bodies, as appropriate.
* Working with the SLT to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
* Ensuring that online safety is integrated with other appropriate school policies and procedures.

The key responsibilities for all members of staff are:

* Contributing to the development of online safety policies.
* Reading the school Acceptable Use Policies (AUPs) and adhering to them.
* Taking responsibility for the security of school systems and data.
* Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
* Modelling good practice when using new and emerging technologies
* Embedding online safety education in curriculum delivery wherever possible.
* Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
* Knowing when and how to escalate online safety issues, internally and externally.
* Being able to signpost to appropriate support available for online safety issues, internally and externally.
* Maintaining a professional level of conduct in their personal use of technology, both on and off site.
* Taking personal responsibility for professional development in this area.

In addition to the above, the key responsibilities for staff managing the technical environment are:

* Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
* Taking responsibility for the implementation of safe security of systems and data in partnership with the SLT.
* To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
* Ensuring that the school’s filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
* Ensuring that the use of the school/setting’s network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
* Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
* Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
* Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
* Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
* Ensuring that the school’s ICT infrastructure/system is secure and not open to misuse or malicious attack.
* Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

The key responsibilities of children and young people are:

* Contributing to the development of online safety policies.
* Reading the school’s Acceptable Use Policies (AUPs) and adhering to them.
* Respecting the feelings and rights of others both on and offline.
* Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

* Taking responsibility for keeping themselves and others safe online.
* Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
* Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

The key responsibilities of parents and carers are:

* Reading the school’s Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
* Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
* Role modelling safe and appropriate uses of technology and social media.
* Identifying changes in behaviour that could indicate that their child is at risk of harm online.
* Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
* Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

***Online Communication and Safer Use of Technology***

**Managing the school’s website**

* The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
* The contact details on the website will be the school’s address, email and telephone number. Staff or pupils’ personal information will not be published.
* The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
* The website will comply with the school’s guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
* The administrator account for the school website will be safeguarded with an appropriately strong password.
* The school will post information about safeguarding, including online safety, on the school website for members of the community.

**Publishing images and videos online**

* The school will ensure that all images and videos shared, are used in accordance with other school policies, such as Safeguarding, Data Protection and Record Management.
* The school will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies and Safeguarding. Written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

**Managing email**

* All members of staff are provided with a specific school/setting email address to use for any official communication.
* The use of personal email addresses by staff for any official school business is not permitted.
* The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
* Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
* Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality, data protection and safeguarding.
* Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school’s safeguarding file.
* Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents.
* Email sent to external organisations should be written carefully and professionally, and may need authorisation before sending, in the same way as a letter written on school headed paper would be.
* School email addresses and other official contact details will not be used for setting up personal social media accounts.

**Official videoconferencing and webcam use for educational purposes**

The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity. At this time, we will not be supporting this type of activity in school.

**Appropriate and safe classroom use of the internet and any associated devices**

* Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
* The school’s internet access will be designed to enhance and extend education.
* Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
* All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
* Supervision of pupils will be appropriate to their age and ability.
* At Early Years Foundation Stage and Key Stage 1 pupils’ access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils’ age and ability.
* 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. Children will be directed to online material and resources which support the learning outcomes planned for the pupils’ age and ability.
* All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
* Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
* Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
* The school will use age appropriate search tools e.g. <http://www.swiggle.org.uk/> <http://www.dkfindout.com/uk/> <http://primaryschoolict.com/>
* The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
* Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**Management of school learning platforms/portals/gateways**

* Leaders/managers and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
* Pupils/staff will be advised about acceptable conduct and use when using the LP.
* Only members of the current pupil, parent/carers and staff community will have access to the LP.
* All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
* When staff, pupils’ etc. leave the school their account or rights to specific school areas will be disabled.

***Social Media Policy***

**General social media use**

* Expectations regarding safe and responsible use of social media will apply to all members of the Lenham Primary School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multi­player online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
* All members of the Lenham Primary School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
* Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the Lenham Primary School community.
* All members of the Lenham Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
* The school/setting will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.
* The use of social networking applications during school hours for personal use **is** permitted by staff only during the lunch break, but cannot be accessed by the school network.
* Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
* Any concerns regarding the online conduct of any member of the Lenham Primary School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
* Any breaches of the school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

**Official use of social media**

* Lenham Primary School has a social media presence on Twitter (@LenhamPrimary)
* Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
* Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
* Staff will use school provided email addresses to register for and manage any official approved social media channels.
* Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
* All communication on official social media platforms will be clear, transparent and open to scrutiny.
* Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
* Official social media use will be in line with existing policies including anti-bullying and child protection.
* Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy and with permission from the parent / careers.
* Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
* Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school/setting website and take place with written approval from the SLT.
* Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
* Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and l action taken to safeguard the community.
* Official social media channels will link back to the school website and/or Acceptable Use Policy to demonstrate that the account is official.
* The school/setting will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

**Staff personal use of social media**

* The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
* Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school’s Acceptable Use Policy.
* All members of staff are advised not to communicate with or add as ‘friends’ any current or past children/pupils or current or past pupils’ family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.
* If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
* All communication between staff and members of the school community on school business will take place via official approved communication channels e.g. through the school’s phone number or school email addresses.
* Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher.
* Any communication from pupils/parents received on personal social media accounts will be reported to the school’s DSL.
* Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
* All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
* All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies (**safeguarding, confidentiality, data protection etc**.) and the wider professional and legal framework.
* Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
* Members of staff will notify the SLT immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
* Members of staff are encouraged not to identify themselves as employees of Lenham Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
* Members of staff will ensure that they do not represent their personal views as that of the school’s on social media.
* School email addresses will not be used for setting up personal social media accounts.
* Members of staff who follow/like the school’s Twitter account, are advised to have ‘locked’ profiles, and user names which cannot be recognised by parents.

**Staff official use of social media**

* If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
* Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
* Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
* Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
* Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so.
* Staff using social media officially will inform the SLT, the Designated Safeguarding Lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.
* Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
* Staff using social media officially will sign the school’s social media Acceptable Use Policy.

**Pupils use of social media**

* Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
* Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
* Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
* Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult’s permission and only when they can be present.
* Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
* Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
* Parents will be informed of any official social media education with pupils.
* Any concerns regarding pupils’ use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
* Any concerns regarding pupils’ use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

***Use of Personal Devices and Mobile Phones***

**Rationale regarding personal devices and mobile phones**

* The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the Lenham Primary School community to take steps to ensure that mobile phones and personal devices are used responsibly.
* The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use documents.
* Lenham Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools/settings.

**Expectations for safe use of personal devices and mobile phones**

* All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies (particularly Safeguarding).
* Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. 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 certain areas within the school - such as toilets.
* The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Behaviour policy.
* Staff will use a work phone number when contacting parents.
* All members of the Lenham Primary School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
* All members of the Lenham Primary School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school’s policies.
* School mobile phones and devices must always be used in accordance with the Acceptable Use Policy.
* School/setting mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

**Pupils’ use of personal devices and mobile phones**

* Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
* Pupils who need to bring a mobile phone to school, will need to take it to office at morning registration time and collect it at the end of the school day.
* Pupil’s personal mobile phones and personal devices will be kept in a secure place and switched.
* If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team and with parental permission.
* If a pupil needs to contact his/her parents/carers they will ask a member of staff to do so on their behalf.
* Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
* If a pupil 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 parents/carers when the adult is able to collect the device.
* School staff may confiscate a pupil’s mobile phone or device if they believe it is being used to contravene the school’s behaviour or bullying policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with the school’s policy and <https://www.gov.uk/government/publications/searching-screening-and-confiscation> ***)***
* If there is suspicion that material on a pupil’s personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

**Staff use of personal devices and mobile phones**

* Members of 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. Any pre-existing relationships which could compromise this will be discussed with SLT.
* Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
* Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
* Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
* Staff personal mobile phones and devices will be switched off/switched to ‘silent’ mode during lesson times, unless ‘special / emergency circumstances’ have been agreed with a member of the SLT.
* Bluetooth or other forms of communication should be “hidden” or switched off during lesson times.
* Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
* If a member of staff breaches the school’s policy then disciplinary action will be taken.
* If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
* Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school’s relevant policies

**Visitors’ use of personal devices and mobile phones**

* Parents/carers and visitors must use mobile phones and personal devices in accordance with the school’s acceptable use policy and guidelines issued on arrival.
* Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
* The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
* Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

***Policy Decisions***

**Reducing online risks**

* Lenham Primary School is aware that the internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
* Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
* The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. The network is provided by EiS and is IWF approved.
* 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 always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
* The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

**Internet use throughout the wider school community**

* The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site

**Authorising internet access**

* All staff and pupils at Lenham Primary School are granted access to the school’s devices and systems.
* All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
* Parents will be informed that pupils will be provided with supervised internet access which is appropriate to their age and ability.
* Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
* When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

***Engagement Approaches***

**Engagement and education of children and young people**

* An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
* Education about safe and responsible use will precede internet access.
* Pupils input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
* Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
* All users will be informed that network and internet use will be monitored.
* Online safety (e-Safety) will be included in the PSHE and Computing programmes of study, covering both safe school and home use.
* Acceptable Use expectations and Posters 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 within all subject areas.
* External support will be used to complement and support the schools internal online safety (e-Safety) education approaches.

**Engagement and education of children and young people considered to be vulnerable**

* Lenham Primary School is aware that some children may be considered to be more vulnerable online due to a range of factors.
* The school will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

**Engagement and education of staff**

* The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
* Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
* 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 in a variety of ways, on a regular (at least annual) basis.
* 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.

**Engagement and education of parents and carers**

* Lenham Primary School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
* Parents’ attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.
* A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent consultations, fetes and sports days.
* Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
* Parents will be encouraged to role model positive behaviour for their children online.

***Managing Information Systems***

**Managing personal data online**

* Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
* Full information regarding the schools approach to data protection and information governance can be found in the schools information security policy.

**Security and Management of Information Systems**

* The security of the school information systems and users will be reviewed regularly.
* Virus protection is updated regularly, through EiS.
* Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
* 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.
* The school’s data capacity is reviewed regularly.
* The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
* All users will be expected to log off or lock their screens/devices if systems are unattended.

**Password policy**

* All users will be informed not to share passwords or information with others and not to login as another user at any time.
* Staff must always keep their password private and must not share it with others or leave it where others can find it. Pupils’ unique passwords are kept secure by them, but can be retrieved by staff if an individual forgets it.
* All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.

**Filtering and Monitoring**

* The governors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children’s exposure to online risks.
* The school’s internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
* All monitoring of school owned/provided systems will take place to safeguard members of the community.
* All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
* The school uses educational filtered secure broadband connectivity which is appropriate to the age and requirement of our pupils.
* The school uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
* The school will work with EiS to ensure that filtering policy is continually reviewed.
* The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
* If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated 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 Leadership Team.
* All changes to the school filtering policy will be logged and recorded.
* The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
* Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

**Management of applications (apps) used to record children’s progress**

* The headteacher is ultimately responsible for the security of any data or images held of children.
* Apps/systems which store personal data will be risk assessed prior to use.
* Only school issued devices will be used for apps that record and store children’s personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children’s personal details, attainment or images.
* Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
* Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
* Parents will be informed of the schools expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

**Responding to Online** **Incidents and Safeguarding Concerns**

* All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
* All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
* The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
* The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
* Complaints about internet misuse will be dealt with under the School’s complaints procedure.
* Complaints about online/cyber bullying will be dealt with under the School’s anti-bullying policy
* Any complaint about staff misuse will be referred to the head teacher
* Any allegations against a member of staff’s online conduct will be discussed with the LADO (Local Authority Designated Officer).
* Pupils, parents and staff will be informed of the schools complaints procedure (website or through the school office)
* Staff will be informed of the complaints and whistleblowing procedure.
* 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.
* 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.
* The school will manage online safety (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 as 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 Education Safeguards Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm.
* 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.
* If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
* If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Kent.
* Parents and children will need to work in partnership with the school to resolve issues.

***Appendix A***

***Procedures for Responding to Specific Online*** ***Incidents or Concerns***

***Responding to concerns regarding Youth Produced Sexual Imagery or “Sexting”***

* Lenham Primary School ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as “sexting”).
* The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers and will be focused on keeping oneself safe online.
* Lenham Primary School views “sexting” as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (Anji Martin)
* The school will follow the guidance as set out in the non-statutory UKCCIS advice ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ <https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis> and KSCB “Responding to youth produced sexual imagery” guidance <http://www.kscb.org.uk/guidance/online-safety>
* If the school are made aware of incident involving creating youth produced sexual imagery the school will:
* Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
* Immediately notify the DSL.
* Store the device securely.
* Carry out a risk assessment in relation to the children(s) involved.
* Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
* Make a referral to children’s social care and/or the police (as needed/appropriate).
* Put the necessary safeguards in place for children e.g. offer support and immediate protection and offer appropriate pastoral support for those involved.
* Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
* Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
* Inform parents/carers about the incident and how it is being managed.
* The school will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
* The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
* If an indecent image has been taken or shared on the school’s network or devices, then the school will take action to block access to all users and isolate the image.
* The school will take action regarding creating youth produced sexual imagery, regardless of the use of school’s equipment or personal equipment, both on and off the premises.
* The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

**Responding to concerns regarding Online Child Sexual Abuse and Exploitation**

* Lenham Primary School will ensure that all members of the community are made aware of online child sexual abuse, including: exploitation and grooming, and the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
* The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
* Lenham Primary School regards online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (Anji Martin).
* If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
* If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSET team (<http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/cse> ) by the DSL.
* If the school are made aware of an incident involving online child sexual abuse of a child then the school will:
	+ Act in accordance with the school’s child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
	+ Immediately notify the DSL.
	+ Store any devices involved securely.
	+ Immediately inform Kent police via 101 (using 999 if a child is at immediate risk)
	+ Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: [www.ceop.police.uk/safety-centre/](http://www.ceop.police.uk/safety-centre/)
	+ Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
	+ Make a referral to children’s social care (if needed/appropriate).
	+ Put the necessary safeguards in place for pupil(s) e.g. offer support and immediate protection and offer appropriate pastoral support for those involved.
	+ Inform parents/carers about the incident and how it is being managed.
	+ Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
* The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
* The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
* If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
* The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button on the school website homepage and on intranet systems.

**Responding to concerns regarding Indecent Images of Children (IIOC)**

* Lenham Primary School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
* The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
* The school will take action to prevent access / accidental access to Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software. (EiS)
* If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
* If the school is made aware of Indecent Images of Children (IIOC) then the school will:
	+ Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Board’s procedures.
	+ Immediately notify the school Designated Safeguard Lead.
	+ Store any devices involved securely.
	+ Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
* If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
	+ Ensure that the Designated Safeguard Lead is informed.
	+ Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](https://www.iwf.org.uk/) .
	+ Ensure that any copies that exist of the image, for example in emails, are deleted.
* If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:
	+ Ensure that the Designated Safeguard Lead is informed.
	+ Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](https://www.iwf.org.uk/) .
	+ Ensure that any copies that exist of the image, for example in emails, are deleted.
	+ Inform the police via 101 (999 if there is an immediate risk of harm) and children’s social services (as appropriate).
	+ Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
* If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
	+ Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
	+ Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
	+ Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
	+ Follow the appropriate school policies regarding conduct.

**Responding to concerns regarding radicalisation and extremism online**

* The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils (EiS monitor access to the network, and alert the school to any possible concerning material).
* When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
* Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.

**Responding to concerns regarding cyberbullying**

* Cyberbullying, along with all other forms of bullying, of any member of the Lenham Primary School community will not be tolerated. Full details are set out in the school policies regarding anti­-bullying and behaviour.
* All incidents of online bullying reported will be recorded.
* There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
* If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
* Pupils, staff and parents/carers will be advised to keep a record of cyberbullying 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 schools e-Safety ethos.
* Sanctions for those involved in online or cyberbullying may include:
	+ Those involved will be asked to remove any material deemed to be inappropriate or offensive.
	+ A service provider may be contacted to remove content if those involved refuse to or are 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 involved in online bullying will be informed.
	+ The Police will be contacted if a criminal offence is suspected.

**Responding to concerns regarding online hate**

* Online hate at Lenham Primary School will not be tolerated. Further details are set out in the school policies regarding anti­-bullying and behaviour.
* All incidents of online hate reported to the school will be recorded.
* All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
* The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

***Appendix B***

***Online Safety (e-Safety) Contacts and References***

***Kent Support and Guidance***

* **Kent County Councils Education Safeguards Team**:
 [www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding)
* **Kent Online Safety Support for Education Settings**
* Rebecca Avery, Education Safeguarding Adviser (Online Protection)
* Ashley Assiter, e-Safety Development Officer
* esafetyofficer@kent.gov.uk Tel: 03000 415797
* **Kent Police:**
[www.kent.police.uk](http://www.kent.police.uk) or [www.kent.police.uk/internetsafety](http://www.kent.police.uk/internetsafety)

 Inan emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

* **Kent Public Service Network (KPSN):** [www.kpsn.net](http://www.kpsn.net)
* **Kent Safeguarding Children Board (KSCB):** [www.kscb.org.uk](http://www.kscb.org.uk)
* **Kent e–Safety Blog**: [www.kentesafety.wordpress.com](http://www.kentesafety.wordpress.com)
* **EiS -** ICT Support for Schools and Kent Schools Broadband Service Desk**:** [www.eiskent.co.uk](http://www.eiskent.co.uk)

***National Links and Resources***

* **Action Fraud:** [www.actionfraud.police.uk](http://www.actionfraud.police.uk/)
* **BBC WebWise:** [www.bbc.co.uk/webwise](http://www.bbc.co.uk/webwise)
* **CEOP (Child Exploitation and Online Protection Centre):** [www.ceop.police.uk](http://www.ceop.police.uk)
* **ChildLine:** [www.childline.org.uk](http://www.childline.org.uk)
* **Childnet:** [www.childnet.com](http://www.childnet.com)
* **Get Safe Online:** [www.getsafeonline.org](http://www.getsafeonline.org/)
* **Internet Matters:** [www.internetmatters.org](http://www.internetmatters.org)
* **Internet Watch Foundation (IWF):** [www.iwf.org.uk](http://www.iwf.org.uk)
* **Lucy Faithfull Foundation:** [www.lucyfaithfull.org](http://www.lucyfaithfull.org)
* **Know the Net:** [www.knowthenet.org.uk](http://www.knowthenet.org.uk)
* **Net Aware:** [www.net-aware.org.uk](http://www.net-aware.org.uk)
* **NSPCC:** [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)
* **Parent Port:** [www.parentport.org.uk](http://www.parentport.org.uk)
* **Professional Online Safety Helpline:** [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)
* **The Marie Collins Foundation:** <http://www.mariecollinsfoundation.org.uk/>
* **Think U Know**: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
* **Virtual Global Taskforce**: [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com)
* **UK Safer Internet Centre:** [www.saferinternet.org.uk](http://www.saferinternet.org.uk)
* **360 Safe Self-Review tool for schools:** <https://360safe.org.uk/>
* **Online Compass (Self review tool for other settings):** <http://www.onlinecompass.org.uk/>

***Appendix C***

***Input from our pupils***

**Internet Safety**

Digital communication can be very dangerous.

There are three important things you must remember when you are online.

**Zip it**

The most important thing you need to know is never share any of your personal information online, especially your address or your school. The reason why you don’t do this is because you never know who you are talking to.

**Block it**

If someone online is being very rude and saying stuff to you that you don’t like, you can always block them.

**Flag it**

Also if you don’t like what they are putting you can flag it. Flag it means it will get read of it straight away, so you can’t see it anymore. When you flag it, it will report the person as well.

It is very important that you tell an adult if there is anything online you don’t like. Always remember treat people how you would like to be treated.

By Robyn

****

**E-Safety**

E-Safety is an essential life skill that will help you a great deal. It will help so much and will keep you safe, because not everyone is lovely and kind on the internet.

Zip It

Zip it is one of the most helpful things on the internet for keeping safe. It is extremely important that you do not share any personal information. Such as: Your phone number; your email address: passwords for social media accounts and others.

**Flag It**

**Flag it is a good feature because you can report any inappropriate content or language in comments. If you flag something or report something it will be sent to moderators for them to look at. Remember, if something makes you upset on the internet, flag it then show a parent or guardian.**



**Block It**

**Block it means that you block a user or profile. This makes it so they cannot see any of your posts or messages. It also blocks their communications to your account. If something is inappropriate make sure to tell an adult then block or vice versa**

**Written By Jake**

***Acceptable Use Policy***

**What is an ‘Acceptable Use Policy’?**

The school encourages and promotes the positive use of ICT to develop curriculum and learning opportunities, as well as promoting personal enjoyment and achievements for all members of the community. It is essential that the use of ICT and online tools are carefully managed by educational settings to ensure that all members of the community (including their data) are kept safe and that online risks and dangers are recognised by the setting and mitigated. AUP (Acceptable Use policies) should be an integral and essential part of this process.

An AUP …

* Is a clear and concise document, which gives all users an outline of acceptable and unacceptable behaviours
* Should be developed with children, staff and parents
* Is appropriate to the school’s community
* Will be part of a pupil or member of staff’s induction
* Is developed by the IT Leader and SLT
* Encourages all members of the school’s community to develop responsibility for their behaviour and practice online
* States what monitoring takes place
* Outlines the sanctions for unacceptable use
* Explains what someone should do if they have a concern
* Signposts users to school, or outside, support

AUPs will be reviewed annually and will reflect any changes to the setting or requirements. They should also be updated in response to any incidents, new technologies or the school’s infrastructure. Any amendments must be shared with all stakeholders.

# Pupils: Acceptable Use Policy

# Early Years Foundation Stage and KS1

*The following points will be taught during Reception Class, Year 1 & Year 2:*

* I only use the internet when an adult is in the room with me.
* I won’t only click on links and buttons, when I don’t know what they do.
* I keep my personal information and passwords safe online and do not share them.
* I only send messages online which are polite and friendly.
* I know the school can see what I am doing online.
* I know that if I do not follow the rules then there will be consequences.
* I have read and talked about these rules with my parents/carers.
* I always tell an adult/teacher if something online makes me feel unhappy or worried
* I can visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) to learn more about keeping safe online

**Key points included on posters in my classroom and in the IT Suite**

* I only go online with a grown up
* I am kind online
* I keep information about me safe online
* I tell a grown up if something online makes me unhappy or worried

****

# Pupils: Acceptable Use Policy

# Key Stage 2 Pupils

*The following points will be taught during Years 3, 4, 5 & 6 and are given as guidance for home and school use:*

* I always ask permission from an adult before using the internet.
* I only use websites and search engines that my teacher has chosen.
* I use my school computers for work at school, unless I have permission otherwise.
* I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult.
* I always credit the person or source that created any work, image or text I use.
* I only talk with and open messages from people I know and I only click on links if I know they are safe.
* I always talk to an adult if I’m not sure about something or if something happens online that makes me feel worried or frightened, and I will immediately turn the screen off.
* I only send messages which are polite and friendly, and with an adult’s knowledge.
* I keep my personal information safe and private online.
* I will keep my passwords safe and not share them with anyone.
* I will not access or change other peoples’ files or information.
* I will only post pictures or videos on the internet if they are appropriate and if I have permission.
* I will only change the settings on the computer if an adult has given me permission.
* I understand that the school’s internet filter is there to protect me, and I will not try to bypass it.
* I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.
* I know that my use of school devices/computers and internet access will be monitored.
* I know that if I do not follow the rules then there will be consequences.
* I have read and talked about these rules with my parents/carers.
* If I am aware of anyone being unsafe with technology then I will report it to an adult.
* I can visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) and [www.childline.org.uk](http://www.childline.org.uk) to learn more about keeping safe online

**Key points included on posters in my classroom and in the IT Suite**

* I will keep information about me and my passwords private.
* I will not be unkind to anyone online.
* If someone online asks me to meet them, I will always talk to an adult straight away.
* I know that people online are strangers and they may not always be who they say they are.
* I know there are laws that stop me copying online content.
* I will always talk to an adult if I see something online which upsets me.
* I know I must only open online messages that are safe and if I’m unsure then I won’t open it without speaking to an adult first.
* I will not assume information online is true.
* I will ask an adult which websites I can use.
* I will not use technology to be unkind to people.

****

**Parent/Carers: Acceptable Use Policy**

* I have read and discussed the Acceptable Use Policy (attached) with my child.
* I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school.
* I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the school’s systems. This monitoring will take place in accordance with data protection and human rights legislation.
* I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task.
* I understand that if the school has any concerns about my child’s safety online, either at school or at home, then I will be contacted.
* I will inform the school, or other relevant organisations, if I have concerns about my child’s safety online.
* I understand that if my child does not abide by the school Acceptable Use Policy then sanctions may be applied in line with the school’s Behaviour and Anti-Bullying policies. If the school believes that my child has committed a criminal offence then the Police will be contacted.
* I, together with my child, will support the school’s approach to online safety (e-Safety) and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
* I know that I can speak to my child’s teacher or the Head Teacher if I have any concerns about online safety (e-Safety).
* I will visit the school website (http://www.lenham.kent.sch.uk) for more information about the school’s approach to online safety, as well as to access useful links to support both myself and my child in keeping safe online at home *(see ‘Online Safety Policy – including Acceptable Use’).*
* I will visit:

[www.thinkuknow.co.uk/parents](http://www.thinkuknow.co.uk/parents),

[www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety),

[www.internetmatters.org](http://www.internetmatters.org)

[www.saferinternet.org.uk](http://www.saferinternet.org.uk)

[www.childnet.com](http://www.childnet.com) for more information about keeping my child(ren) safe online.

* I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

**I have read the Parent / Carers: Acceptable Use Policy**.

Child’s Name……………………………………………………………………. Class…………………………

Parent’s Name……………………………………………........ Parent’s Signature……………………………

Date…………….

***Note: Please be aware that if parents/carers refuse to sign and agree the AUP then this can cause issues as children will need to use the internet in order to access the curriculum.***

**Letter to parents/carers re: online safety**

Dear Parent/Carer,

All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

* Computers, laptops and other digital devices
* Internet, which may include age-appropriate search engines and educational websites
* The school’s network
* Games consoles (e.g. Wii, but this is not internet enabled)
* Digital cameras and video cameras
* Recorders and Dictaphones

Lenham Primary School recognises the essential and important contribution that technology plays in promoting children’s learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed an Online Safety Policy and procedures alongside the school’s safeguarding measures. *(Please see the policy via the school’s website).*

The school takes your child’s online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. However, no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the internet. The school is not liable for any damages arising from use of the schools internet and ICT facilities.

We request that all parents/carers support the school’s approach to online safety by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers can visit the school website’s, <http://www.lenham.kent.sch.uk/> for more information about the school’s approach to online safety, as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit;

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk),

[www.childnet.com](http://www.childnet.com),

[www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety),

[www.saferinternet.org.uk](http://www.saferinternet.org.uk) and

[www.internetmatters.org](http://www.internetmatters.org) for more information about keeping children safe online.

Whilst the school monitors and manages technology use in school, we believe that children themselves have an important role in developing responsible online behaviours. In order to support the school in developing your child’s knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child and that you and your child discuss the content and return the attached slip. Hopefully, you will also find the Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

Should you wish to discuss the matter further, please do not hesitate to contact the school.

**For Reception, Year 1 and Year 2 Pupils**

We understand that your child is too young to give informed consent on his / her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

Yours sincerely,

Ms Howell

**Letter to Staff re: Online Safety & Acceptable Use Policy**

Dear xxxxx

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of both your professional reputation and that of the school when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be “private” and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, personal contact details, video or images etc online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don’t be afraid to be yourself online, but do so respectfully. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.

If you have a social networking account, it is advised that you do not to accept pupils (past or present) or their parents/carers as “friends” on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. Contact with pupils and parents should only be through school email (preferably via the office email address) and telephone numbers. This is essential in order to protect yourself, as well as the wider community. If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns about this, then please speak to the headteacher (myself) or the Designated Safeguarding Lead (Anji Martin).Please book an appointment to do this before the end of November 2016.

## Documents called “[Cyberbullying: advice for headteachers and school staff](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf)” <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf> and “Safer professional practise with technology” <http://www.kelsi.org.uk/__data/assets/pdf_file/0004/60934/Safer-Practice-August-2016.pdf> are available online and may help you to consider how to protect yourself online. Staff can also visit, or contact the Professional Online Safety Helpline [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline) for more advice and information on online professional safety.

I would like to remind all staff of our updated ‘Online Safety Policy – including Acceptable Use Policy’ (October 2016), as keeping yourself and others safe online, is more than just your use of social media.

Failure to follow this guidance and the school policy could lead to disciplinary action, so it is crucial that all staff are aware of the policy’s contents.

Please speak to any member of the SLT, of Ceri Norey, in her role as Chair of Governors, if you are unsure of any of the points raised in this letter, or in the policies.

Yours sincerely,

Headteacher

# Staff: Acceptable Use Policy 2016

# *Kent County CouncilAs a professional organisation with responsibility for children’s safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school’s computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.*

# *This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.*

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**
2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
4. I will respect system security and I will not disclose any password or security information. I will use a ‘strong’ password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly – at least once a year).
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.
7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. I will protect the devices in my care from unapproved access or theft.
8. I ensure any personal information stored on the school computer system, including any school laptop or similar device issued to members of staff, is only stored temporarily and is able to be accessed in the event of an investigation.
9. I will respect copyright and intellectual property rights.
10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
11. I will report all incidents of concern regarding children’s online safety to the Designated Safeguarding Lead (Anji Martin) and/or the headteacher, as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the SLT, DSL and IT technician.
12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the IT Technician, Liz Waller.
13. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Headteacher.
14. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems.  This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school’s Online Saftey Policy – including Acceptable Use Policy, and the law.
15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the DSL or SLT.
18. I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

*The School may exercise its right to monitor the use of ~~i~~nformation systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the schools information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.*

**I have read and understood and agree to comply with the Staff Acceptable Use Policy.**

Signed: …………………………………….... Print Name: ………………….……………… Date: ……….…

Accepted by: ……………………………….… Print Name: ……………………………….…. Date: …….……

# Kent County CouncilVisitor/Volunteer: Acceptable Use Policy

# *For visitors/volunteers and staff who do not access school ICT systems*

# *As a professional organisation with responsibility for children’s safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.*

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.
2. I have read and understood the school ‘Online Safety Policy – including Acceptable Use’, which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
3. I will follow the school’s policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.
5. My use of ICT and information systems will be compatible with my role within school.  This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law
6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
8. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Anji Martin) or the Head Teacher.
9. I will report any incidents of concern regarding children’s online safety to the Designated Safeguarding Lead as soon as possible.

**I have read and understood and agree to comply with the Visitor /Volunteer Acceptable Use Policy.**

Signed: ……………………………..………. Print Name: ………………………………… Date: …….……

Accepted by:…………………………………. Print Name: ………………………………… Date: …….……

# *Kent County Council*Wi-Fi Acceptable Use Policy

# For those using the school’s Wi-Fi

# *As a professional organisation with responsibility for children’s safeguarding it is important that all members of the school community are fully aware of the school’s boundaries and requirements when using the school Wi-Fi system, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that IT use should be consistent with the school ethos, other appropriate policies and the Law.*

Please be aware that the Lenham Primary School will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the school.

The school provides Wi-Fi for the school community and allows access for visiting professional and those who have a pre-arranged letting agreement with the school, which includes mention to access.

1. The use of IT devices falls under Lenham Primary School’s ‘Online Safety Policy – including Acceptable Use’, ‘Behaviour Policy’, ‘Data Protection’ and ‘Safeguarding’, which all students/staff/visitors and volunteers must agree to, and comply with.
2. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
3. School owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
4. I will take all practical steps necessary to make sure that any equipment connected to the school’s service is adequately secure (such as up-to-date anti-virus software, systems updates).
5. The school’s wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school’s wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.
6. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school’s wireless service’s connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.
7. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school’s wireless service.
8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
9. I will not attempt to bypass any of the schools security and filtering systems or download any unauthorised software or applications.
10. My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
11. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
12. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Anji Martin) or the SLT, including the headteacher, as soon as possible.
13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the SLT.
14. I understand that my use of the schools Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation*.* If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

**I have read and understood and agree to comply with Lenham Primary School’s Wi-Fi Acceptable Use Policy.**

Signed: ……………………………..………. Print Name: ………………………………… Date: …….……

Accepted by:…………………………………. Print Name: ………………………………… Date: …….……

#  Kent County CouncilStaff Social Networking Acceptable Use Policy

# *For use with staff running official school social media accounts*

1. As part of the school’s drive to encourage safe and appropriate behaviour in the use of today’s technology, I will support the school’s approach to online safety. I am aware that Twitter is a public and global communication tool and that any content posted may reflect on the school, its reputation and services. I will not use the site to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.
2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school’s SLT. The SLT and Governing Body retain the right to remove or approve content posted on behalf of the school.
3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
4. I will follow the school’s policy regarding confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy.
5. I will promote online safety (e-Safety) in the use of Twitter and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by a member of senior leadership team / Designated Safeguarding Lead /head teacher prior to use.
6. I will set up a specific account / profile using a school provided email address to administrate the Twitter account and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school’s SLT will have full admin rights to the Twitter account.
7. Where it believes unauthorised and /or inappropriate use of the Twitter, or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.
9. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the head teacher and/or Designated Safeguarding Lead urgently.
10. I will ensure that the Twitter account is moderated on a regular basis as agreed with the Governing Body.
11. I have read and understood the school ‘Online Safety Policy – including Acceptable Use’, which covers the requirements for safe IT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the SLT.
12. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the SLT.

I have read and understood and agree to comply with the School Social Networking Acceptable Use policy.

Signed: ……………………….... Print Name: ……………………… Date: ………

Accepted by: ……………………………. Print Name: ………………………….