Repton Manor
Primary School

E-Safety Policy
October 2017

Policy lead	Kayleigh Simpson
Date approved by Governing Body	October 2017
Governor signature	
Review date	October 2018

This policy in a working document which includes all Acceptable Use Policies to encapsulate the roles and responsibilities for all members of the Repton Manor community. In this way, we hope to ensure that we are all appropriately educated in how to safely and responsibly use digital resources.

Repton Manor Primary School believes that online 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 understand 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.

The purpose of Repton Manor Primary School 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 Repton Manor Primary School is a safe and secure environment.
- Safeguard and protect all members of Repton Manor Primary School community online.
- Raise awareness with all members of Repton Manor Primary School 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.

Staff and Governors Acceptable Use Policy

As 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.

- 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. Given this information, I understand all school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.

- School owned information systems must be used appropriately and I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- 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.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (containing both letters and numbers) and change this at least once every academic year. 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.

- 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 password protected. 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. You can find whether there is parental consent for sharing photos on SIMS or can ask or a class list from the office.

- 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.. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment (if appropriate) or via VPN. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I understand that this Acceptable Use Policy is one of seven for various stakeholders in the school and the others can be found in the online safety Policy.

- I understand that it is my role to ensure children are appropriately supervised when using ICT in accordance with age and SEND. I will ensure that I use positive role modelling to encourage safe use of technology and continue to teach children about e-safety with the guidance of the computing curriculum lead. 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.

- I will always proof view any content which I am due to show to children or recommend viewing at home.

- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Matt Rawling / Kayleigh Simpson) as soon as possible on a pink slip. This includes any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites. I will identify individuals of concern and take appropriate action by following school safeguarding policies and procedures.

- 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 ICT Support Provider as soon as possible.

- 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. I recognise that I am only advised to respond to parents/professionals during working hours and communication with other staff will be in line with our minimum standards. 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.

- 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.

- I will ensure that my online reputation and use of ICT 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 ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

- 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. This is inclusive of both personal and professional devices including social media and mobile phones. 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.

- I will attend yearly safeguarding and e-safety training and seek additional support if I feel that it would be beneficial to the children in our school. I understand that the training will enable me to know when and how to escalate online safety issues, internally and externally. And appropriately signpost to appropriate support available for online safety issues. If I have any further 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 (Kayleigh Simpson / Matt Rawling)

- 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. I am 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.

- I recognise that I am 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 Head Teacher. If ongoing contact is required, this should be done using school approved communication.

- I will not use inappropriate or excessive use of social media during work hours or whilst using school devices and understand this may result in disciplinary or legal action and/or removal of Internet facilities.

- I will not share any information on any children, families or staff on social media sites.

- I understand that I am encouraged not to identify myself as an employee of Repton Manor Primary School on my 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.

- I understand that electronic devices of all kinds that are brought in on site are my responsibility and 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 only permitted in areas of the school which are private and where there are no children present. It is the staff members responsibility to ensure that there are no personal electrical devices around the children unless at the discretion of Senior Leadership Team. I will protect my phone with a confidential password to ensure that unauthorised calls or actions cannot be made if it is lost or stolen.

- I will confiscate a pupil's mobile phone or device if I believe it is being used to contravene the schools behaviour or bullying policy or could contain youth produced sexual imagery (sexting). I will not view any images suspected of being youth produced sexual imagery and will liaise with the Designated Safeguarding Lead immediately.

- 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.

- I will not take photos of children on any personal device, nor will I use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

- I will only use school issued devices for apps that record and store children's personal details, attainment or photographs. I will not use my personal devices to access or upload content to any apps which record and store children's personal details, attainment or images.

- I will challenge visitors and parents to our school who are using mobile phones around school, if I have continuing concerns, I will report these to the DSL. Before any school production, I will make parents aware that they must not post photos of other people children to any social media sites.

The School may exercise its right to monitor the use of information 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: …………………………

Designated Safeguarding Lead Acceptable Use Policy

- I understand that I am a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- I understand that it is my responsibility to implement and review the e-safety policy and procedures (including acceptable use policy), at least annually. This will be ratified by Governors and communicated to all stakeholders in the school. I will know who the named Governor for e-safety is.
- I will ensure that through regular training (at least annually), updates, induction and communication that online safety is viewed by the whole community as a safeguarding issue. This includes working with the curriculum lead to ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- I will ensure 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
- I will ensure that the training covers safe and responsible Internet use, both professionally and personally.
- I will ensure that I have appropriate time, training and to fulfil my online safety role and responsibilities and that I am keeping up-to-date with current research, legislation and trends regarding online safety.
- I will work with technical staff to monitor the safety and security of the school system and networks.
- I will 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. These systems are also in place to prevent staff and pupils from accessing unsuitable or illegal content.
- I will ensure that staff and children are aware that they should report unsuitable sites to me and I will ask for the site to be blocked.
- I will be aware of any online safety incidents, recording them appropriately and ensuring that external agencies and support are liaised with as appropriate, in line with Kent Safeguarding Children's Board thresholds and procedures (See Appendix A). If I am unsure how to proceed with any incidents of concern, then I will escalate the incident to the Education Safeguarding Team.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately. 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.
- I will raise any complaint about staff misuse to the Head Teacher and ensure that any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- I will receiving and regularly reviewing online safeguarding records and practice and using them to inform and shape future practice, identifying strengths and areas for improvement.
- I will ensure that the computing lead has undertaken appropriate risk assessments regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- I will monitor the curriculum lead in co-ordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

- As Designated Safeguarding Lead, I will ensure that our practice for data protection and data security is in line with current legislation.
- I am aware that I am the dedicated email for reporting wellbeing and pastoral issues.
- I will assume that all staff and pupils will have access to the schools devices and systems and maintain a current record of all staff and pupils who are not for any period of time.
- I will ensure that procedure is in place for all staff, pupils, parents and visitors to read and sign the Acceptable Use Policy before using any school resources.
- When considering access for vulnerable members of the community (such as with children with special education needs) I will ensure the school makes decisions based on the specific needs and understanding of the pupil(s).
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- I will draw parents attention to online safety (e-Safety) policy and expectations in newsletters, letters and on the school website.

- I will ensure that we work together with parents regarding any concerns surrounding e-safety and 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.
- Parents and staff will be informed of the schools complaints procedure at their request and through the school website.
- Staff will be informed of the complaints and whistleblowing procedure.

I am responsible for ensuring that the school and Governors will follow and understand the procedures below;

- 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 uses educational filtered secure broadband connectivity through the KPSN 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 KCC and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
- 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.

I have read and understood and agree to comply with the Designated Safeguarding Lead Acceptable Use Policy.

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

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

Curriculum Lead Acceptable Use Policy

- I will ensure that online safety is embedded within a progressive whole School curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- I will ensure Internet use is a key feature of educational access which is designed to enhance and extend education 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.

- I understand that some children may be considered more vulnerable online due to a range of factors, these include children identified as SEND. I will ensure that learning is differentiated with input from specialist staff as appropriate (Inclusion Leader and Pastoral Support Manager)
- I will ensure that education about safe and responsible use will precede internet access.
- I will ensure the school will use age appropriate search tools.
- Through the curriculum and teaching, I will ensure that pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- I will ensure the evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-School requirement across the curriculum.
- Emerging technologies will be examined for educational benefit and I will present these to SLT with appropriate risk assessments.
- I will ensure pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- I will ensure online safety (e-Safety) education and training will be included as part of the transition programme across year groups and for children transitioning in year.
- I will ensure Acceptable Use expectations, posters and routines are embedded in all areas with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas, covering both safe school and home use.
- I will ensure the school rewards positive use of technology by pupils.
- I will highlight, through training, useful online tools which staff should use according to the age and ability of the pupils.
- I will make Information and guidance for parents on online safety available to parents in a variety of formats.

I have read and understood and agree to comply with the Curriculum Lead Acceptable Use Policy.

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

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

Repton Manor
Primary School

Network Lead Acceptable Use Policy

- I will provide a safe and secure technical infrastructure which will support safe online practices while ensuring that learning opportunities are still maximised.
- I will take responsibility for the implementation of safe security of systems and data in partnership with the Senior Leadership Team.
- I will provide suitable access controls and encryption to protect personal and sensitive information held on school-owned devices.
- I will ensure that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL. I will work with KCC and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually followed and will block all sites on the Internet Watch Foundation (IWF) list.

- I will ensure that the use of the School's network by staff and children is regularly monitored and will report any deliberate or accidental misuse immediately to the DSL. I will then work with them to ensure that they are recorded and appropriate action is taken as advised.
- I will have an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure and advise Senior Leaders of how to ensure this is implemented the school if necessary.
- I will report any breaches and liaise with Senior Leaders and the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- I will provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- I will ensure that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack. This includes, ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- I will ensure the school uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our pupils.
- I will ensure 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.
- I will remove links and block sites as directed by the school Senior Leadership Team.
- 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.
- I will work with staff to monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
- I will ensure that only members of the current pupil, parent/carers and staff community will have access to the school networks or devices.
- I will advise the school of any issues that may breach copywrite law regarding use of ICT.
- I will ensure when staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled or (if appropriate) transferred to their new establishment.
- The security of the school information systems and users will be reviewed regularly.
- Files held on the school's network will be regularly checked.
- As technical lead for Repton Manor Primary school I will advise of suitable provision for disaster recovery, backing up of data and reviewing system capacity regularly.
- I will work with the school to ensure that the information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- I will only publish materials to the school website when agreed with the Senior Leadership Team.
- I will ensure that the administrator account for the school website will be safeguarded with an appropriately strong password.

I have read and understood and agree to comply with the Network Lead Acceptable Use Policy.

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

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

Repton Manor
Primary School

Parents and Carers Acceptable Use Policy

Repton Manor Primary School recognise that parents/carers have an essential role to play in enabling children to be safe and responsible users of the internet and digital technology. We will endeavour to draw your attention to e-safety and expectations in newsletters, letters and on the school website. In addition, we will endeavour to provide education, to both you and your child about keeping safe online. By working in partnership with you, we are able to protect your children better and prepare them for a safe future. We ask that you are aware of and sign to agree to the following guidance on keeping children safe when using a variety of technologies.

- 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 schools 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. At home I will ensure that I have taken all reasonable steps to ensure that my child only accesses appropriate materials; these will include computer games.
- 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 understand that if my child does not abide by the school 'Acceptable Use Policy' then sanctions will be applied in line with the schools behaviour and anti-bullying policy. 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 understand that I am not able to use mobile phones or personal devices around the school site. I also understand that I am not able to post photos of other people's children to social media sites.
- I know that I can speak to the school Designated Safegurding Lead (Kayleigh Simpson or Matt Rawling) if I have any concerns about online safety (e-Safety).
- I will visit the school website (http://www.reptonmanorprimary.co.uk/learn/e-safety) 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.
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and 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 and Carers Acceptable Use Policy.

Child's Name……………………………………………… Class……………………….

Parents Name…………………………………………………Parents Signature…………………………………….

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. Schools must have a robust process in place to manage and record parental responses and also to engage with parents who do not respond. Alternatives include highlighting online safety (e-Safety) within the Home School Agreement and an acknowledgement form for the AUP.

Repton Manor
Primary School

Early Years and KS1 Acceptable Use Policy

- I only use the internet when an adult knows that I am on it.
- I only click on links and buttons when I know what they do
- I do not share my personal information and passwords.
- 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 the school may speak to my parents / carers and I may get a yellow / red card or not be allowed on the computers.
- I have read and talked about these rules with my parents/carers

- I always tell an adult if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online

Name……………………………………………………………………………….

Date……………………………………………………………………………….

Repton Manor
Primary School

KS 2 Acceptable Use Policy

- I know that I will be able to use the internet in school, for a variety of reasons, if I use it responsibly. However, I understand that if I do not use it responsibly, I may not be allowed to use the internet at school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it immediately to an adult in school or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by never telling anyone I meet online my address, my telephone number, my school's name, or my surname or by sending a picture of myself without permission from a teacher or other trusted adult.
- I will never arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude or bullying emails, pictures or messages I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check with an adult in the school before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.

- If I bring in memory sticks / CD ROMs from outside of school I will always give them to my teacher so they can be checked for viruses and content, before opening a file.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal e-mail, social networking sites or instant messaging in school.
- If, for any reason, I need to bring my mobile phone into school I know that it is to be handed in to the office and then collected at the end of the school day.
- I will tell a teacher or other trusted adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online
- I understand that if the school or my parents or carers are worried, they will look through my phone, computer, tablet or electronic devices to ensure I am safe.
- I understand that I must show an adult any images before I send them to someone I trust.

I have read and understood the Acceptable Use Policy.

Name: ………………………………………………………………………………………………. Date: ……………………………….

Repton Manor
Primary School

Visitor/Volunteer Acceptable Use Policy

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.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998 and remains on site at all times.

- I understand that I have a duty to supervise children when they are accessing Information Communication Technology

- 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.

- I will not share any information in the capacity of my role regarding the school, children, staff or families on any social media sites.

- 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

- 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.

- 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.

- 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 (Kayleigh Simpson / Matt Rawling).

- I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Kayleigh Simpson / Matt Rawling) immediately.

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

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

Accepted by:………………………….. …………Date: ……………..

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- Repton Manor 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.
- Repton Manor Primary School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Leads (Matt Rawling or Kayleigh Simpson).
- 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' and KSCB "Responding to youth produced sexual imagery" guidance
- 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 designated safeguarding lead.
  - 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 counselling 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 Schools 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 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

- Repton Manor Primary School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including 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.
- Repton Manor Primary School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (*Matt Rawling and Kayleigh Simpson*).
- 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 by the DSL.
- If the school are made aware of incident involving online child sexual abuse of a child then 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 designated safeguarding lead.
    - 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/
    - 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 counselling 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.

Responding to concerns regarding Indecent Images of Children (IIOC)

- Repton Manor 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 equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to of 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.
- 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 Boards 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 .
    - 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 .
    - 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.
- 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 Repton Manor 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

- 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

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 or www.kent.police.uk/internetsafety

In an 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

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

Kent e–Safety Blog: www.kentesafety.wordpress.com

EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

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

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

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

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: 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/