Roseberry Primary School
R P S

Policy for E- Safety

Approved by the Governing Body:	**October 2015**
Interim Review:	**September 2016**
Review Date:	**September 2017**
Head teacher:	**Maggie Fearnley**

New technologies have become fundamental to the lives of children and young people in today's society, both in and outside school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication can help teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective, independent learning.

Children and young people should have an entitlement to safe internet access at all times. At Roseberry, it is our duty to ensure that children and young people are able to use the internet and related communications technologies appropriately, and safety is addressed as part of the wider duty of care to which all who work in schools are bound.

Our school e-Safety policy should help to ensure safe and appropriate use of the Internet and electronic equipment, at all times. The development and implementation of such a strategy will involve all stakeholders - from the head teacher and governors, to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers children may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyberbullying;
- Access to unsuitable video/internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build pupils' awareness and resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks appropriately. Roseberry will aim to educate its pupils in safeguarding themselves; equipping children with the skills they need to ensure that they can do everything that is reasonably expected of them, to manage and reduce these risks.

This e-Safety policy aims to highlight how we, at Roseberry, intend to do educate and protect its pupils, while also addressing wider educational issues, in order to help young people (and their parents/carers) to be responsible users and stay safe, while using the internet and other communications technologies, for educational, personal and recreational use.

This Policy should be read in conjunction with the following school policies:
- Safeguarding Policy
- Health and Safety Policy
- Acceptable Use Policy & Computing Policy
- Whole School Behaviour Policy

Who is responsible for e-safety?

The Staff of Roseberry are responsible for ensuring that:

- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices;
- they have read, understood and signed the school Staff Acceptable Use Agreement (AUP)
- they report any suspected misuse or problem to the e-Safety Co-ordinator/Head teacher;
- digital communications with pupils (e-mail) should be on a professional level and only carried out using DB Primary;
- e-Safety issues are embedded in all aspects of the curriculum and other school activities;
- pupils understand and follow the school e-Safety and Acceptable Use Policy,
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor IT activity in lessons, extra-curricular and other school activities;
- they are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current acceptable use with regard to these devices;
- in lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

The e-Safety lead should be trained in e-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyberbullying.

Pupils, taking into account the age and level of understanding, should:

- be responsible for using the school IT systems in accordance with the Pupil Acceptable Use Agreement (AUP), which they and/or their parents/carers will be expected to sign before being given access to school systems;
  However, at EYFS and KS1 it would be expected that parents/carers would sign on behalf of the pupils.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- expect to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyberbullying;
- understand the importance of adopting good e-Safety practice when using digital technologies out of school.

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.
Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy (AUP);
- accessing the school website in accordance with the relevant school Acceptable Use Policy.
- ensuring that they themselves do not use the internet/social network sites/other forms of technical communication in an inappropriate or defamatory way.

Teaching and Learning

Why Internet use is important

- Internet use is part of the statutory IT curriculum and is a necessary tool for learning.
- The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

How Internet use enhances learning

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

How pupils will learn how to evaluate Internet content

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing published content

We have created a website that inspires pupils to publish work of a high standard. We use it to celebrate pupils work, promote the school and publish resources for projects. Publication of information should be considered from a personal and school security viewpoint.
The website will comply with current guidelines for publications including respect for intellectual property rights and copyright.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- Email addresses will be published carefully online, to avoid being harvested for spam.
- The IT coordinator will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, pupils and parents/carers need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images can remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

The school will inform and educate users about these risks and will teach pupils, as appropriate, to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; **the personal equipment, including cameras and mobile phones, of staff should not be used for such purposes**.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute, e.g. swimming.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that includes pupils, will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (signed by parents or carers at the start of the pupil's school career).
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Managing social networking, social media and personal publishing sites

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.

Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published..

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with pupils, as part of the curriculum, will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain consent from the Headteacher before using Social Media tools in the classroom, e.g. using a mock Facebook account to show children how to manage their privacy settings.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- 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.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
- Teachers cannot under any circumstances mention any references to their working lives on any social media.
- Staff personal use of social networking, social media and personal publishing sites guidelines will be issued as part of staff induction and outlined in the school Staff Acceptable Use Policy
- A sample advice leaflet for parents on Social Networking Sites, in particular, Facebook, should be issued to parents when and where appropriate

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the Staff Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read and sign the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site, who require access to the schools network or internet access, will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

At Key Stage 1, pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.

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.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–safety policy is appropriate. Methods to identify, assess and minimise risks will be reviewed regularly.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias, Racist or Misleading info or Advice
Contact (Child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers, Being groomed	Self-harm, Unwelcome Persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information/advice

Byron Review (2008)

Responding to incidents of concern

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material
- criminally racist material
- other criminal conduct, activity or materials

then staff should complete the Incident Record Log.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Person for Child Protection will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection Policy for dealing with concerns.
- The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy, where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learned and implement any changes required.
- Any racist incidents will be reported to the headteacher and a 'racist incident form' should be completed
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Local Authority Designated Officer (LADO) – see Child Protection Policy.

Managing Mobile Phones and Personal Devices

- The use of mobile phones and other personal devices by pupils and staff in school is outlined in the Safe Code of Conduct and covered in the School Acceptable Use policy, and includes:
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- Mobile phones and personal devices **are not** permitted to be used in certain areas within the school site such as the children's, toilets.

Pupils' use of personal devices:
If a pupil brings a mobile device to school 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 at the end of the school day.

Staff use of personal devices:

- Staff **are not** permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- For school visits, staff will be issued with a school phone where contact with parents/carers or the school is required.
- Mobile phones and devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods or at any time where children may be present, e.g. morning time.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Introducing the policy

Useful e–safety programmes to use, when introducing the policy to **pupils**, include:

Think U Know: www.thinkuknow.co.uk
Childnet: www.childnet.com
Kidsmart: www.kidsmart.org.uk
Orange Education: www.orange.co.uk/education
Safe: www.safesocialnetworking.org

- All users will be informed that network and Internet use will be monitored.
- An e–safety programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- e-Safety rules and copies of the pupil Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

Discussing the policy with staff

- The e–safety Policy will be formally provided to all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- 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.

Enlisting parents' support

- Parents' attention will be drawn to the school e–safety Policy on the school website.
- A partnership approach to e-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 e–Safety at other attended events e.g. parent evenings, class assemblies and sports days.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read and sign the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, which include responsible use of the Internet, will be made available to parents on the school website

Pupil Acceptable Use Policy

These rules will help us to be fair to others and keep everyone safe.

I will only use IT in school for school purposes.

I will only use my own school DB Primary e-mail address when e-mailing others within school.

I will only open e-mail attachments from people I know, or who my teacher has approved.

I will not tell other people my passwords.

I will only open/delete my own files.

I will make sure that all IT contact with other children and adults is responsible, polite and appropriate.

I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone that I have made contact with over the Internet.

I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.

I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

I know that my use of IT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

Signed: _____

Date: _____

Pupil Acceptable Use – Pupil and Parent/Carer Agreement

Dear Parent/ Carer,
IT, including the internet, e-mail and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any form of IT.
Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page.
If you have any concerns or would like some explanation please contact Mrs Fearnley.

Parent/Carer signature
We have discussed this and …… (child name) agrees to follow the e-Safety rules and to support the safe use of ICT at Roseberry Primary School

Signed: _____(parent/carer)

Date: _____

Name of Child:_____

Class/Teacher: _____

STAFF / GOVERNOR/ VISITOR ACCEPTABLE USE POLICY AGREEMENT

IT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. This applies to IT used in school and also applies to use of school IT systems and equipment out of school and use of personal equipment in school or in situations related to their employment by the school.

All staff/Governors/visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Linda Hollinshead (e-Safety lead) or Maggie Fearnley (Head Teacher).

- I will only use the school's email/Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head teacher
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) such as DB Primary or SBC School email account for any school business.
- I will ensure that personal data (such as data held in SIMS and the school's network) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware of software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes using school equipment, in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support and promote the school's e-Safety, Data Protection and Behaviour policies and help pupils to be safe and responsible in their use of IT and related technologies.
- I will not use mobile phones or other personal electronic/hand held devices in the presence of children.

I understand this forms part of the terms and conditions set out in my contract of employment.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines. I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Name: _____

Signed: _____

Position: _____

Date: _____

SOCIAL NETWORKING SITES - FACEBOOK
GUIDANCE FOR PARENTS/CARERS

There are many children of Primary School age who have Facebook Profiles despite the permitted minimum age to use the site being 13, according to the siteterms and conditions.

Our school is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this particular issue as a concern. Whilst children cannot access Facebook or other social networking sites at school, they could have access to it on any other computer or mobile technology. Websites such as Facebook offer amazing communication and social connections, however, they are created with their audience in mind and this is specifically 13 years old.
Possible risks for children under 13 using the site may include:

- Facebook use 'age targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered;
- Children may accept 'friend requests' from people they don't know in real life which could increase the risk of inappropriate contact or behaviour;
- Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children;
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own;
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and other options;
- Facebook could be exploited by bullies and for other inappropriate contact;
- Facebook cannot and does not verify its members therefore it important to remember that if your child can lie about who they are online, so can anyone else!

We feel that it is important to point out to parents/carers the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from school and sometimes by a child, their friends, siblings or even parents.
We will take action (such as reporting aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children.

Should you decide to allow your children to have a Facebook profile we strongly advise you to:

- Check their profile is set to private and that only 'friends' can see information that is posted;
- Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting offensive messages or photos;
- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a bookmark on their profile to CEOP and the 'Report Abuse' button which has been known to deter offenders;
- Have a look at the advice for parents/carers from Facebook www.facebook.com/help/?safety=parents;
- Set up your own profile so you understand how the site works and ask them to add you as a friend on their profile so you can keep track of what they are posting online;
- Make sure your child understands the following rules:
    - Always keep your profile private;
    - Never accept friends you don't know in real life;
    - Never post anything which could reveal your identity;
    - Never post anything you wouldn't want your parents to see;
    - Never agree to meet someone you only know online without telling a trusted adult;
    - Always tell someone if you feel threatened or someone upsets you.

We recommend that all parents/carers visit the CEOP ThinkUKnow website for more information on keeping your child safe online.

RESPONSE TO AN INCIDENT OF CONCERN
E-SAFETY INCIDENT LOG

Details of e-Safety incidents to be recorded by staff and passed on to the e-Safety Coordinator. This incident log will be monitored termly by the Head teacher.

Date/Time	Name of Pupil or Staff Member	Room and Computer	Details of Incident (including Evidence)	Actions and Reasons

Signed: _____Date: _____