Roseberry Primary School
R P S

Policy for Internet Safety
(Online Safety)

Approved by the Governing Body:	**October 2016**
Interim Review:	**September 2021**
Review Date:	**September 2022**
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 Internet 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 Internet 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
(Sending Nudes) Sexting Policy

Who is responsible for Internet Safety?

Governors:

Governors are responsible for the approval of the Internet Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about internet safety incidents and monitoring reports in line with monitoring and sharing of safeguarding information. As members of the Governing Body, their role will include:

- regular monitoring of Internet Safety incident logs
- regular monitoring of filtering/change control logs
- discussing aspects of Internet Safety at committee meetings

Head Teacher and Senior Leaders:

- The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community
- The Head Teacher and Computing/Online Safety Lead should be aware of the procedures to be followed in the event of a serious Internet Safety allegation being made against a member of staff.
- The Head Teacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Designated Safeguarding Person:

The Head Teacher (DSP) and Deputy Headteacher (Deputy DSP) should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- o Sharing of personal data
- o Access to illegal/inappropriate materials
- o Inappropriate on line contact with adults/strangers
- o Potential or actual incidents of grooming
- o Cyberbullying, sexting, radicalisation and other Internet Safety issues.

Lead:

- leads the online safety and computing team
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Internet Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with the Head Teacher and Governors to discuss current issues, review incident logs and filtering/change control logs
- reports regularly to Senior Leadership Team

The online safety lead will be trained in online safety issues and will be aware of the potential for serious child protection issues to arise from:

- o Sharing of personal data
- o Access to illegal/inappropriate materials
- o Inappropriate online contact with adults/strangers
- o Potential or actual incidents of grooming
- o Cyberbullying, sending nudes (sexting), radicalisation and other online safety issues.

The Staff of Roseberry are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online 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 Head Teacher and the Computing/online safety lead for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using Roseberry Primary Year Group email
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school Online 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 online 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.

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 and peer on peer abuse
- understand the importance of adopting good Internet 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

Network Manager/Technical staff (ONEITSS) are responsible for ensuring:

- that our school's technical infrastructure is secure and is not open to misuse or malicious attack
- that our school meets required Internet Safety technical requirements and any Local Authority Internet Safety Policy/ guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with Internet Safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network/Internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head Teacher and Online Safety Lead

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

Educating Pupils on the Importance of Online Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the Roseberry Primary School's Digital Literacy and Internet Safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. Our current Digital Literacy (online safety) curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A progressive online safety curriculum is provided as part of the Digital Literacy and Computing Curriculum, PHSE, maths, English and topic lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the Internet and mobile devices
- In lessons where Internet use is pre-planned, it is best practice that 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
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the technical staff (at ONEITSS) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and the Online Safety Lead should be made aware of such requests before they take place.

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.

Educating Parents and Carers on the Importance of Internet Safety

Some parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website,
- Parents/Carers Family Time sessions and meetings
- High profile events and campaigns e.g Safer Internet Day
- Reference to the relevant web sites/publications (including electronically via our school Website/Facebook and Twitter pages)

Educating the Wider Community on the Importance of Internet Safety

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and Internet Safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
  Supporting community groups e.g Early Years Settings, sports groups to enhance their online safety provision

Education and Training of Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.   It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g from LA/ other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be with staff in staff meetings/INSET days.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Education and Training of Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are involved in health and safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association or other relevant organisation
- Participation in school training/information sessions for staff

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that Roseberry Primary meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- The Online Safety Lead and LA officer is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. *An appropriate system is in place (Incident Log) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data, and are tested regularly.
- o The school infrastructure and individual workstations are protected by up to date virus software
- An agreed username and password (which restricts access to the school network) is in place for the provision of temporary access of "guests" (e.g trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured.

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 information about our school, policies and practices. 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, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies 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.
- Parents and carers are not permitted to take videos and digital images of their children at school events for their own personal use (GDPR) to respect everyone's privacy and in some cases, to protect vulnerable children.
- 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 (following written and signed consent from parents). Images should only be taken on school equipment. The personal equipment of staff, including cameras and mobile phones, is not permitted 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 our school website, Facebook or Twitter pages, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images (and consent from parents).
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

Communication Technologies to Enhance Learning

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how Roseberry Primary currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras				✓				✓
Use of other (school owned) mobile devices e.g iPads, iPods	✓						✓	
Use of other personal mobile devices e.g iPads, iPods, gaming devices or tablets				✓				✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of messaging apps in lessons				✓				✓
Use of social media in lessons		✓ with prior permission from HT or ES Lead						✓
Use of blogs (the school blogsite)	✓				✓			

When using communication technologies, Roseberry Primary School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access). DB Primary for children. DB primary and SBC schools for staff
- Users must immediately report, to the Head Teacher or Online Safety Lead, in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- **Any digital communication between staff and pupils or parents/carers (email) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will be provided with individual log ins for Seesaw, Mathletics, Reading Plus and Times Tables Rockstars
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

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 pupils, 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, will be issued to parents when and where appropriate

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Roseberry Primary School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- **They do not accept friend requests from pupils, both current and past pupils, parents or carers.**

The school's use of social media for professional purposes will be checked regularly by the Head Teacher and Online Safety Lead to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video guidelines as outlined by this policy.

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 IT 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 school's 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 Roseberry Primary School nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
The school will audit IT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate. Methods to identify, assess and minimise risks will be reviewed regularly.

	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)

Unsuitable/Inappropriate Activities

Roseberry Primary 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. This policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the Internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing				X		
Use of social media (with prior permission from Head Teacher or Internet Safety Lead for purposes of educating children about privacy settings)			X			
Use of messaging apps					X	
Use of video broadcasting e.g Youtube			X			

Responding to Incidents of Misuse or Concern

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see 'User Actions' above).

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 report these to the Headteacher and complete the Incident Record Log immediately.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Online Safety Coordinator will record all reported incidents and actions taken in the Online Safety incident log and other in any relevant areas e.g. Bullying or Safeguarding log (CPOMS).
- The Head Teacher (Designated Person for Child Protection) will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Safeguarding Policy for dealing with concerns.
- Online Safety incidents will be managed in accordance with our school's behaviour policy, where appropriate.
- We will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the Head Teacher or Online Safety Lead will debrief, identify lessons learned and implement any changes required.
- Any racist incidents will be reported to the Head Teacher 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 Safeguarding Policy.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow our school Online Safety policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate Internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below.
- Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action

- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that Roseberry Primary staff will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures. The following tables will indicate the nature or reporting and sanctions:

Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email					X		X	
Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another student's / pupil's account	X	X			X		X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's / academy's filtering system					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X

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 this policy as well as 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 when on school trips or for taking images/videos of children.

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 Internet Safety Policy

Useful online 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 online 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.
- Online 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 Online safety and technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

Discussing the policy with staff

- This Online 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 Online Safety Policy 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 attended events e.g. parent evenings, class assemblies, Family Time and sports days.
- Parents will be requested to sign an Online 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 Online 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 Online 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 Online 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 Online Safety rules and to support the safe use of IT 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 (Online 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 IT 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 or parents/carers.
- 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 Online Safety , Data Protection, Sexting, Radicalisation 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 IT 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 site terms 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
INTERNET SAFETY INCIDENT LOG

Details of Internet Safety incidents to be recorded by staff and passed on to the Internet Safety Lead. 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: _____________________________