Roseberry Primary School

R P S

Acceptable Use Policy and Agreements

Approved by the Governing Body:	**October 2016**
Interim Review:	**September 2020**
Review Date:	**September 2022**

Purpose

To allow appropriate and reasonable use of electronic media and services, including computers, e-mail, on live services, the school network, the internet and hand-held devices by the pupils and staff of Roseberry Primary School.

To encourage the creative and safe use of these media associated services through clear but proportionate guidelines to benefit our school, pupils' learning, teaching and home lives.

All employees and everyone connected with our school should remember that electronic media and services provided by Roseberry are Roseberry's property and their primary purpose is to facilitate and support teaching and learning. Therefore, all users have the responsibility to use their resources in a professional, ethnical and lawful manner.

Internet

Access to the internet is a vital part of life here at Roseberry Primary School, and as such, a higher level of internet access must be given to staff to ensure they are able to work effectively and efficiently. Staff internet access is filtered to reduce any inappropriate sites being visited. Staff must be vigilant in what they are accessing on the internet and must not access or attempt to access any sites that contain any of the following; child abuse, pornography, promoting discrimination in any kind of way; promoting racial or religious hatred, promoting or having links to extremist groups, promoting illegal acts; any other information which may be illegal or offensive to colleagues.

If a member of staff inadvertently accesses any website or internet service that could be classed as inappropriate, they should report it to Maggie Fearnley (Head teacher), Linda Hollinshead (IT Lead) and OneItss - our IT systems manager - immediately.

Prohibited communications

Electronic media must not be used for transmitting, retrieving or storing any communication that is;

- Discriminating or harassing
- Derogatory to any individual or group
- Obscene, sexually explicit or pornographic
- Defamatory or threating
- In violation of any licence governing the use of software
- Engaged in for any purpose that is illegal or contrary to the school policy or interests.

Personal use

The computers, electronic media and services provided by the school is primarily for educational use to assist and enhance teaching and learning. Limited, occasional or incidental use of electronic media (sending or receiving), the internet or the computers for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not adversely affect the systems use for their educational purposes. However, employees are expected to demonstrate a sense of responsibility and not to abuse this privilege.

Roseberry can check all usage history of its internet connection and network but will not do so unless it feels there is a need to do so.

Personal computers and mobile devices must have a password and must not be left unlocked when unattended.

Accessing School WI-FI and the school network

Only devices that have been checked with the IT department are authorised to be used to connect to the school WI-FI and network. Any device that connects to the school network via WI-FI or a wired connection should have the latest updates including security patches and have valid and up to date anti-virus software installed. Also, devices should not contain any material that is inappropriate within a school environment.

There are many WIFI points around school: Where are they? The WIFI is called ……. And all school devices can be connected to it.

Any visitors to the school should not be connected to the school WI-FI.

Removable devices; USB sticks, SD cards, external hard drives and storage devices.

Removable devices such as SD cards and external hard drives may be connected to the school network. Memory cards or memory sticks are not permitted.

If you suspect a device to be damaged, to contain inappropriate material or a virus, do not connect it to any school device including computers, photocopiers, laptops, cameras and phones. The device should be given to Linda Hollinshead at the earliest opportunity who will safely store it before giving it to ONEItSS to check and approve its use.

Access to employee communications

Electronic communication/information created is done so through an employee using email, word processing, utility programmes, spread sheets, internet and bulletin board systems and is not reviewed by the school. However, Roseberry routinely gathers logs for the most electronic activities and monitors employee communications directly e.g. internet logs, space on server, integrity of files.

The school reserves the right, as its discretion, to review any employees electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law. Employees should not assume electronic communications or electronic files are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

Software

To ensure that Roseberry is compliant with software licensing and to prevent computer viruses from being transmitted through the schools computer system, unauthorised downloading of any software is strictly prohibited. Any software requirements can be discussed with ONEItSS who will authorise the software installation or organise the purchasing of software licenses where applicable.

Security/ appropriate use

Employees must respect the confidentiality of other individuals electronic communications, except for cases whereby explicit authorisation has been granted by school management. Employees are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees or third parties.
- Hacking or obtaining access to systems or accounts they are not authorised to use.
- Using other people's log-ins or passwords.
- Breaching, testing or monitoring computer or network security measures.

No email or other electronic communications may be sent that attempt to hide the identity of a sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network or congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic access to other companies or individuals materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Anyone receiving in appropriate contact from parents, past parents, pupils or past pupils should inform the head immediately.

Participation in online forums

Employees should remember that any messages of information sent on school provided facilities to one of more individuals via an electronic network- for example online services - are statements identifiable and attribute to Roseberry Primary school.

Roseberry recognises that participation in some forums might be important to the performance of an employees job. For instance, an employee might find the answer to a technical problem by consulting members of news group devoted to the technical area.

Social networking sites

The following should be followed by members of staff (employees) and is recommended as best practise for volunteers.

Social networking sites such as: Facebook, YouTube, or Twitter should not be used by employees whilst teaching a lesson or when directly in charge of pupils. It is best practise that staff should not include parents within their 'social networking' as this may lead to compromising the staff/parent professional relationship.

Another danger for staff is posting compromising pictures of themselves on sites that could then be accessed by the public and/or the media. It is imperative that staff maintain professional standards and avoid bringing their profession and the school into dispute.

If staff wish to access social networking sites whilst at work, then this must only be done as part of a reasonable 'break' and on their own personal computer or mobile device (when not in charge of pupils)

Mobile phones

Staff may not use their mobile phone while they are directly in charge of pupils or whilst carrying out their role at Roseberry Primary School, other than in case of emergency or extremely urgent school business when it must be safe to phone.

Personal mobile phones should not be used to photograph, film or record (sound and visual) pupils by members of staff or whilst in capacity of a volunteer.

Personal mobile phones should not be used to phone pupils' personal mobiles or contact pupils directly. If you need to speak to a pupil, then you must phone the pupils parents and gain access to them via their parent or parents.

Photography and filming

All staff and volunteers, whilst in the capacity of a member of staff, are given guidance on Roseberry's policy on using and storing images of children. This includes;

- Staff should ALWAYS use school cameras/recording devices, NOT personal equipment.
- Digital images of children must be stored on the password protected area of the schools network.
- Digital images of pupils should not be stored on personal/home computers/hard drives.
- Hard copies of pupils images should be stored in a locked filing cabinet on the school premises.

Do not download any photographs, film or sound recordings of pupils onto your own personal technology, for example a work station or laptop.

Violations

Any employee who abuses the privilege of their access to the school network email, the internet or other technologies in violation of this policy will be subject to disciplinary action, up to and including possible termination of employment, legal action and criminal liability.

Equipment and passwords

Staff are responsible for the security of their computers, devices and other equipment Roseberry allocates to them. This equipment is not to be used by anyone other then in accordance with this policy.

Passwords are beneficial for us at Roseberry are the confidential property of the school and must be used to secure access to data kept in such equipment, thereby using that confidential data is protected in the event of loss or theft.
If you feel someone else knows your password, please change it immediately. Our systems are set for your password to change periodically and will request you to change your password once it has expired. However, passwords must be changed half term and it is the responsibility of the user to do this.
Passwords should be a complex combination of upper and lowercase case characters, numbers and symbols such as; @! # etc. it is also very good practise to not use common words found in the dictionary or especially using a family members name. Passwords should never be given to other members of staff to 'unlock' classroom computers. It is good practice to log off any school device, including the classroom laptop, when leaving the room.

Pupil Acceptable Use and Agreement: School Devices and Internet

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

- I will only use devices in school for school purposes
- I will only use my own log in details and access my own accounts within school – I will not access or use another child's or adult's credentials
- I will only open/delete my own files
- I will not tell other people my passwords
- I will only use a school email address when e-mailing others within school
- I will only open email attachments from people I know and after checking with them first (to ensure it has been sent from that person)
- I will only access files or open attachments when approved by my teacher
- I will only take photographs or make recordings when asked directly by my teacher or teaching assistant.
- If taking a photograph of another child or adult, I will seek permission from this person beforehand
- I will only access my own accounts, e.g. reading plus and not log in as another child using their private credentials

I will apply my Digital Literacy (Online-Safety) knowledge as taught in lessons and do my part to keep myself and others safe:

- I will make sure that all online or IT contact with other children and adults is responsible, polite and appropriate (THINK: True, helpful, inspiring, necessary and kind).
- I will not deliberately look for, save or send anything that could be unpleasant or unkind. If I accidentally find anything like this, I will tell my teacher or teaching assistant immediately.
- I will not give out my own personal 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 support the school approach to online safety and not deliberately upload, add images, video, sounds or text that could upset any member of my 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 Internet Safety or use.

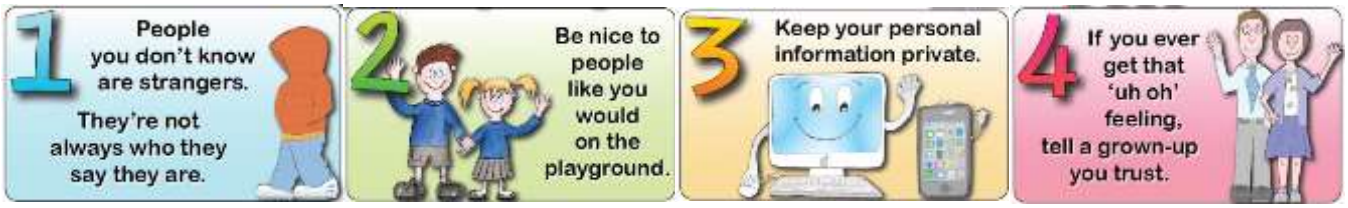
Signature ..... Date .....

Full Name .....

Class .....

Roseberry
Primary School

Online Safety Top Tips!



Remember these 5 SMART rules when using the internet and other mobile devices.

S	SAFE	Keep safe by being careful not to give out personal information to people you are chatting to online. This includes: your full name, email address, phone number, home address, photos or school name.
M	MEET	Meeting someone you have only been in touch with online can be dangerous. Never meet up with anyone unless you are with your parents.
A	ACCEPTING	Accepting emails, messages or opening files, picture or texts from people you don't know or trust can lead to problems. They may contain viruses, unkind messages or inappropriate content.
R	RELIABLE	Information you find on the internet may not be true, or someone online may be lying about who they are. Make sure you check information with a trusted adult before you believe it.
T	TELL	Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

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 the Internet 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 Internet 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 Agreement: School Devices and Internet

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 Acceptable Use Agreement aims 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 (Internet Safety lead) or Maggie Fearnley (Head Teacher).

- I will only use the school's devices for the purpose of teaching and learning and NOT for any **personal use**.
- 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 Office 365/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 Internet Safety, Data Protection, Sexting, Radicisation, Home Learning 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.
- If using a personal computer at home, I will only use 'Remote Access'. If using a school encrypted laptop, I will use Remote Access or my 'offline' folder. This ensures that any personal/confidential data that I produce will be stored within the schools systems and will be kept private.
- I will ensure that any transporting of images from a camera's internal memory or memory card, or iPad's internal memory is done so to a computer/laptop/Applemac/iPad at school, and not transferred to personal electronic devices, either in school or at home.
- I understand that data protection requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's Digital Literacy (Online-Safety) Curriculum into my teaching and capturing of images or recordings made will adhere to our school's Safeguarding, Online Safety and Home Learning policies.
- I understand that all images stored on removal memory cards or the camera's/iPad's internal memory can be viewed by a member of staff at any time, without notice and should be made available on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety and Home Learning policies.

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 including Facebook

Guidance for Parents/Carers

There are many children of Primary School age who have personal profiles on social media sites such as Facebook and Instagram despite the permitted minimum age to use these sites being 13.

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 social media sites, including Facebook, may include:

- use of '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/Instagram or other social media sites 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;
- Social media sites can be exploited by bullies and for other inappropriate contact;
- Facebook/Instagram 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: _____