The Raleigh
E-Safety Policy

February 2017 **to be reviewed February 2018**

E-safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, anti-bullying, data handling and the use of images.

Using this policy

- The school has an e-safety committee (e-safety co-ordinator, IT technician, computing subject leader, DDSL (Deputy Designated Safeguarding Lead) and computing link governor).
- Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by the Leadership Team and approved by governors.
- The e-safety policy was revised by: Sharon Chase
- It was approved by the Governors on: February 2017
- The e-safety policy and its implementation will be reviewed annually. The next review is due: February 2018.
- The e-safety policy covers the use of all technology and devices which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil/guest.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by passwords. See password policy.
- Systems are in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform reviews of this e-safety policy.
- The security of school IT systems will be reviewed regularly.
- The IT technician manages filtering systems and monitors IT. Any issues are passed onto the Headteacher or deputy Headteacher.

Internet Use

The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families will take place using school equipment and/or school accounts.

Pupils will be advised not to give out personal details or information which may identify them or their location.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- Staff to pupil email communication must only take place via a school email address that is specially created for this purpose.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

Published content eg school web site, school social media accounts

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreycc.gov.uk/?a=168635 (currently under review)

Use of social media including the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating children in their use.
- Use of video services such as Skype and Facetime will be monitored and set up only by staff.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Use of personal devices

- Personal devices may be used by staff and/or pupils to access the school IT systems provided their use complies with the e-safety policy and the relevant Acceptable Use Policy (AUP).
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.
- To protect the school's systems, USB sticks brought into school by children or visitors must be scanned first by an adult. This can be done by right clicking on the USB stick icon when in 'My Computer' (when using school Windows system)

Protecting personal data

- The school has a separate Data Handling Policy. It covers access to pupil and staff personal data on and off site and remote access to school systems.

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.

- People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment or accessing the school wifi using their own devices.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy
To pupils

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet.
- Pupils will be reminded about the contents of the AUP as part of their e-safety education.

To staff

- All staff will be shown where to access the e-safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet.
- All staff will receive e-safety training on an annual basis as part of Safeguarding training.

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School e-safety policy in newsletters and on the school web site.
- Parents and will be offered e-safety training annually and the presentations and information will be available on the school web site and attention will be drawn to these in newsletters.

General use of mobile phones and personal devices

- Mobile phones and personally-owned devices may not be used during lessons or formal school time. They should be switched off (or silent) at all times.
- Mobile phones and personally-owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as the changing rooms and toilets.

- Mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with explicit consent from a member of staff and sanctioned by a senior member of the school.
- The Bluetooth functionality (or similar radio data transfer methods) of a mobile phone should not be used to send images or files to other mobile phones.
- Personal mobile devices will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- Parents and other visitors at all school events (including PSA, extra-curricular and sport events) should not take photographs or video footage of children other than their own (apart from other children when there is direct parental consent given at the time). A reminder of this will be given at events and included in event information letters.
- Photographs or video footage of other children taken at school events should not be downloaded onto any social media platform or forwarded electronically to third parties. A reminder of this will be given at events and included in event information letters.
- The following statement is for letters and announcements: Please note, visitors may not take photographs or video of children other than their own, unless direct parental consent has been given at the time. Photographs or film of other children may not be forwarded electronically to third parties or downloaded onto any social media platform.

Pupils' use of personal devices

- Unless there are exceptional circumstances and pupils have agreed to the AUP, pupils' mobile phones are not permitted in school.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with school policy.
- If a pupil needs to contact his or her parents or carers, the school will contact them. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences and encouraged to use PIN's and other security as necessary.
- Pupils will be provided with school mobile phones or other mobile devices to use in specific learning activities under the supervision of a member of staff.

Staff use of personal devices

- Staff should never contact children from their personal mobile phone, or give their mobile phone number to children. If a member of staff needs to make telephone contact with a parent, a school telephone should be used.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required, for example a mobile on school trips or school landline or school office. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where the staff member doesn't have access to a school owned device, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.
- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode and left in a safe place during lesson times.
- Staff use of mobile phones during the school day will normally be limited to the break times and after school.
- Mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the leadership team in emergency circumstances.
- Approval by a member of the leadership team must be explicitly given before children may use mobile phones or a personal device as part of an educational activity. Generally they will be a good educational reason for the activity to take place.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.

- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft, especially if they are using the school email app on their phone.
- Staff should not send and receive texts in classrooms or use camera phones at any time.
- Staff should never store parents' or pupils' telephone or contact details on their mobile phone, as this allows the possibility of inappropriate contact.
- Staff should never send, or accept from anyone, texts or images that could be viewed as inappropriate.
- If a member of staff suspects a message, text or similar may contain inappropriate content it should not be opened but a senior member of staff, preferably the e-safety coordinator or DSL should be contacted.

Student mobile phone acceptable use policy

Purpose
The widespread ownership of mobile phones among young people requires that school administrators, teachers, children, parents and carers take steps to ensure that mobile phones are used responsibly at school. This AUP is designed to ensure that potential issues involving mobile phones can be clearly identified and addressed, ensuring the benefits that mobile phones provide (such as increased safety) can continue to be enjoyed by our children.

The Raleigh has established the following AUP for mobile phones that provides teachers, children, parents and carers guidelines and instructions for the appropriate use of mobile phones during school hours.

Children, their parents or carers must read and understand the AUP as a condition upon which permission is given to bring mobile phones to school.

The AUP for mobile phones also applies to children during extra-curricular activities both on the school grounds and off-site, including during PSA events. Children are not however permitted to take their mobile phones on school day or residential trips.

Rationale
The school recognises that personal communication through mobile technologies is an accepted part of everyday life but that such technologies need to be used appropriately and safety.

Personal safety and security
Our school accepts that parents/carers may give their children mobile phones to protect them from everyday risks involving personal security and safety. There is also increasing concern about children travelling alone on public transport or commuting long distances to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can contact their child if they need to speak to them urgently while the child is travelling between home and school.

Responsibility
It is the responsibility of children who bring mobile phones to school to abide by the guidelines outlined in this document.

The decision to provide a mobile phone to their children should be made by parents or carers. It is incumbent upon parents to understand the capabilities of the phone and the potential misuse of those capabilities.

Parents/carers should be aware if their child takes a mobile phone to school it is assumed parents have the required insurance cover in the event of loss or damage. The school cannot accept responsibility for any loss, damage or costs incurred due to its use.

Parents/carers are reminded that in cases of emergency, the school office remains a vital and appropriate point of contact and can ensure your child is reached quickly and assisted in any relevant way.

Password Policy

All adult users responsible for choosing strong passwords and protecting their log-in information from unauthorized people. The purpose of this policy is to make sure all the school's resources and data receive adequate password protection. The policy covers all users.

Password Creation

- All passwords should be reasonably complex and difficult for unauthorized people to guess.
- In addition to meeting those requirements, adults should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective.
- A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember" can become "TmB0WTr!".

- All passwords must be changed regularly. This requirement will be enforced using software when possible.
- If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.
- Default passwords — such as those created for new users when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

Protecting Passwords

- Users may never share their passwords with anyone else, including IT staff and senior staff. Everyone who needs access to the school's system will be given their own unique password.
- Users may never share their passwords with any outside parties.
- Users should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.
- Users must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.
- Users may not use password managers or other tools to help store and remember passwords without the IT Technician's permission.
- If a password is forgotten then the IT technician can organise a re-set. If staff experience a problem accessing the network and require immediate access and the IT technician is unavailable, rather than using someone else's log-in details, they must use a temporary guest account which will be available from a secure location in the school office.
- It is the user's responsibility to keep their log-in details secure and to lock their workstation when not in use.
- It is the user's responsibility if their username and password have been used inappropriately.

Children's Usernames and Password

- The children should have graduated password training so that they can practice keeping passwords and private information safe and they can learn to understand the importance of this.
- Children in R use a common passcode for ipads.
- Children R and Y1 have a username and simple common password.
- Children in Y2-6 have a username and personal password that has been generated for them that they are unable to change.
- If the security of a pupil's password is in doubt, a new password should be requested and will be re-set by the IT Technician.
- Class teachers have a record of their class's passwords. This must be kept in a secure location and must not be shown or made available to other children.

Acceptable Use Policy for Children's Mobile devices

Children will only bring in mobile phones in exceptional circumstances and further to signing the Acceptable Use Policy. This AUP applies to the school day, extra-curricular activities both on the school grounds and off-site and during PSA events.

Mobile phones will be switched off (not just put on silent mode); left in children's bags, out of sight.

Mobile phones should not be used in any manner or in any location that could cause disruption to the normal routine of the school.

Children should protect their phone numbers. This will help protect the student's number from falling into the wrong hands and guard against insulting, threatening or unpleasant communications.

The school recognises the importance of emerging technologies present in modern mobile phones e.g. camera and video recording, internet access, MP3 and MP4 playback, blogging etc. Teachers may wish to utilise these functions to aid teaching and learning and pupils may have the opportunity to use mobile phones in the classroom. On these occasions, express permission will be given by the leadership team. The use of mobile phones in one lesson for a specific purpose does not mean further usage is then acceptable.

If asked to do so, children will show the content requested or hand their phone to a teacher or other designated adult such as the police.

Theft or damage

Theft or damage responsibility lies with the child; the school accepts no responsibility for replacing lost, stolen or damaged mobile phones.

The school accepts no responsibility for children who lose or have their mobile phones stolen while travelling to and from school.
To reduce the risk of theft during school hours, children who carry mobile phones are advised to keep them well concealed and not 'advertise' that they have them.

When a mobile phone is found on the school premises and the owner cannot be located, it should be handed into the school office.

It is strongly advised that children use passwords and/or pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other children, or if stolen). Children must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.

Lost and stolen mobile phones in the U.K. can be blocked across all networks making them virtually worthless to the thief. Call your network provider as soon as possible after your phone has been lost or stolen. This can be a temporary measure in case it is recovered.

Inappropriate conduct

Using mobile phones to bully or threaten children or staff is unacceptable. Cyberbullying will not be tolerated. In some cases it could constitute criminal behaviour. Using technology to humiliate, embarrass or cause offence will not be tolerated; regardless of whether 'consent' was given.

It is forbidden for children to use their own or other children's mobile phones to take videos and pictures of acts to denigrate or humiliate others. This also includes using mobile phones to photograph or film any child or member of staff without their consent. It is a criminal offence to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced.

Children should not take photographs or film of other children during any school event (this includes PSA events, extra-curricular activities and sport events) and they must not download them onto any social media platform or forward them electronically to others.

Mobile phones are not to be used or taken into changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow pupils, staff or visitors to the school.

Should there be one disruption to lessons caused by a mobile phone, the responsible child may face disciplinary actions as sanctioned by the Headteacher. This may include a mobile phone ban in school.

Any child who uses vulgar, derogatory, or obscene language in school while using a mobile phone will face disciplinary action at the Headteacher's discretion, which could involve the police.

Children must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence. Similarly, 'sexting' – which is the sending of personal sexual imagery - is also a criminal offence.

Sanctions

If the phone is being used inappropriately the student must give it to a teacher if requested.

On any infringement of this policy the mobile phone would be confiscated by the teacher and taken to a secure place within the school office. The parent/carer will be able to collect the mobile phone at the end of the school day and a record will be made of the incident.

If the incident involves children under the age of 13 or is deemed illegal or inappropriate then the school has a duty to inform the Local Area Designated Officer for safeguarding (LADO) and may refer the incident to the police.

Signed (student) _____ date:_____

Print name : _____ class:_____

Signed (parent) _____ date:_____

Print name : _____

Acceptable Use Policy for Staff and Governors

ICT and the related technologies such as email, 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 and governors are aware of their professional responsibilities when using any form of ICT. All staff and governors are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with the e-safety coordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I understand that I am responsible for all activity carried out under my username.

- I will only use the approved, secure email system for any school business.

- I will ensure that all electronic communications with parents, pupils and staff, including email, instant messaging and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.

- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network/learning platform without the permission of the Headteacher.

- I will not install any hardware or software without the permission of the IT Technician.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- I will respect copyright and intellectual property rights.

- 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 my Line Manager or Headteacher.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote e-safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will report any incidents of concern regarding children's safety to the e-safety Coordinator, the Designated Safeguarding Lead or Headteacher.

- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serous infringements may be referred to the police.

- I have read the complete and most recent E-safety Policy.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name…… (Printed)

Job title……

Signature…… Date……

Acceptable Use Policy for Visitors

- I understand that I have been given use of the school internet and/or school ICT systems in order to carry out a specific job for the school.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for the purpose for which I have been given access.
- 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 not install any hardware or software without the permission of the IT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school ICT systems.
- 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 or my employer.
- I will respect copyright and intellectual property rights.
- I understand that if I disregard any of the above then it will be reported to my employer (if appropriate) and serious infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name…… (Printed)

Company……

Signature…… Date……

Acceptable use of the school computers R and KS1	
These rules help me to stay safe on the internet	
	I will take care of the school computers.
	I will only use the internet when I have been given permission by an adult.
	I will tell an adult if I see something on the internet that upsets me or a message pops up that I don't understand.
	I will not tell other people my personal things about me or my passwords.
	I will always be polite and friendly when I write messages on the internet. **I will follow the 'SMART' rules.**

My name: . . . . . Date: . . . . . .

Acceptable use of the school computers KS2

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

- I will only use the school's computers for schoolwork and homework
- I will not tell anyone my login and password
- I will only login to the school systems as myself
- I will only edit or delete my own files
- I am aware that some websites and social networks have age restrictions which mean that I should not go on them
- I will only visit internet sites that are appropriate for my age
- I will only communicate with people I know, or that a responsible adult has approved
- I will only send polite and friendly messages
- I will not open an attachment, download a file or install any software unless I have been given permission by an adult
- If I see any display message on the screen that I don't understand, I will report it to an adult
- I will not change any computer/laptop settings without permission
- I will not tell anyone my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission
- If I see anything I am unhappy with or I receive a message I do not like, I will show a responsible adult.
- I will use technology responsibly
- I will follow the 'SMART' rules.

My name: . . . . . Date: . . . . . .

Parent/Carer Consent Form and E-Safety

All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the e-safety rules have been understood and agreed.

Parent / Carer name: ……

Pupil name: ……..…….

As the parent or legal guardian of the above pupil, I have read and understood the 'Acceptable Use of the School Computers' rules (attached) and grant permission for my daughter or son to have access to use the internet, school email system, learning platform and other ICT facilities at school.

We have discussed the 'Acceptable Use of the School Computers' rules (attached) and my daughter or son agrees to follow these rules and to support the safe and responsible use of ICT at The Raleigh.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using appropriate web filtering for schools, monitored email access, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their e-safety or e-behaviour they will contact me.

I understand the school is not liable for any damages arising from my child's use of the internet facilities.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent/Guardian signature:

……..Date**……**

For your reference a copy of this consent form, 'Acceptable Use of the School Computers' rules for R/KS1 and KS2 can be viewed on the school website as part of the full e-safety policy. The SMART rules are displayed in classrooms and around the school and can also be found on our website.

Please complete, sign and return to your child's class teacher.