Rosendale Primary School and Children's Centre
Rosendale Road, West Dulwich, London SE21 8LR **Tel** 020 8670 4962 **Fax** 020 8761 9997
Email info@rosendale.cc

E-SAFETY POLICY

A statement of Rosendale Primary School's approach to e-safety

Last reviewed: November 2016

Next review: November 2017

SLT owner: Headteacher

Distribution: Governors and staff

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the London Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

E-Safety Audit – Rosendale Primary School

This quick self-audit will help the senior leadership team (SLT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	Y
Date of latest update: February 205	
The Policy was agreed by governors on:	
The Policy is available for staff at: School website	
And for parents at: School office and school website	
The designated Child Protection DSP is: Kate Atkins	
The e-Safety Coordinator is: Rachael Gallagher	
Has e-safety training been provided for both pupils and staff?	Y
Do all staff sign an ICT Code of Conduct on appointment?	Y
Have school e-Safety Rules been set for pupils?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	Y
Has the school filtering policy has been approved by SLT?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

Contents

School e-Safety Policy

The school will appoint an e-Safety coordinator. In many cases this will be the Designated Child Protection Officer as the roles overlap.

Our e-Safety Policy has been written by the school, building on the Sheffield and Kent Children and Young Peoples' Directorates and Government guidance. It has been agreed by the senior leadership team and approved by governors.

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DfE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupil online safety curriculum

Rosendale has a clear, progressive online safety curriculum. This covers a range of skills and behaviours appropriate to their age and experience, covering:

- Content – pupils will understand what appropriate content is and know what to do if they see something inappropriate.
- Contact – pupils will understand not to share personal information with strangers online and what to do if they are contacted by someone they don't know.
- Conduct – pupils will understand how to behave appropriately and safely online and will understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Safe Communication

- Communication received from pupils to any staff member must not be replied to. Emails or messages received through any social media platform must be immediately forwarded to the school e-safety co-ordinator and head of school. Teachers must follow this up by speaking to pupils about why they have not received an emailed response from them.
- Communication between staff members must be professional and appropriate. Staff should be mindful that electronic communication can be requested under the Education Act (2011) and that the act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. Any inappropriate communication will result in staff becoming subject to school disciplinary proceedings.
- The sending of abusive or inappropriate text messages is forbidden.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Each class has a class email address that can be used for supervised whole class correspondence.
- Emails from pupils to staff will not receive a reply, in accordance with the 'safe communication' section of this policy.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

- The forwarding of chain letters is not permitted.

Social Networking

- School will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Photographs and videos will only be uploaded to the school's approved social networking sites (such as YouTube and Twitter) using school or class accounts. Videos will be unlisted and therefore only visible through school website and class blogs.
- In school, pupils are only able to upload and publish within school approved systems, such as class blogs or class Twitter accounts.
- Teachers are instructed not to run social networking spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

Filtering

The school will work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will be issued with a school phone where contact with pupils is required.
- Staff are to use school owned devices only for capturing, recording and storing data or photos of children. With prior permission staff may use own cameras on trips with a school SD card, or a camera phone if photos are deleted once they have been uploaded on return to school.

Published Content and the School Web Site

- The contact details on the website should be the school address, e-mail 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.
- Uploading of information is restricted to our website authorisers.
- The school website complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other work is published or lined to, we credit the sources used and state clearly the author's identity or status.
- Photographs published on the web do not have full names attached

- We do not use pupil's names when saving images in the file names or in the tags when publishing to the school website.

Publishing Pupils' Images, Videos and Work

- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website or blogs in association with photographs or videos.
- Written permission from parents or carers to publish photographs and videos on school websites and blogs will be obtained on enrolment.
- Work can only be published with the permission of the pupil.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Cloud storage

- Google Drive is used by staff and pupils. Google Drive complies with DfE checklist and the EU-US Safe Harbour List. Public sharing is restricted, and pupils are advised never to save their full name in a document or any personal details such as a date of birth or address.
- Evernote is approved by the school for education and assessment purposed. Evernote complies with EU data protection legislation and is on EU-US Safeharbour list. Evernote is encrypted and password protected, and no personal details of children are stored other than first name and surname initial. Eg Joe-H.

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. Neither the school nor Lambeth LA can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-safety Incidents

- A senior member of staff will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- Staff will be alert to and report any incidences that relate to the prevent agenda to a senior member of staff who will take relevant steps.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be educated about e-safety in adherence with the computing National Curriculum.

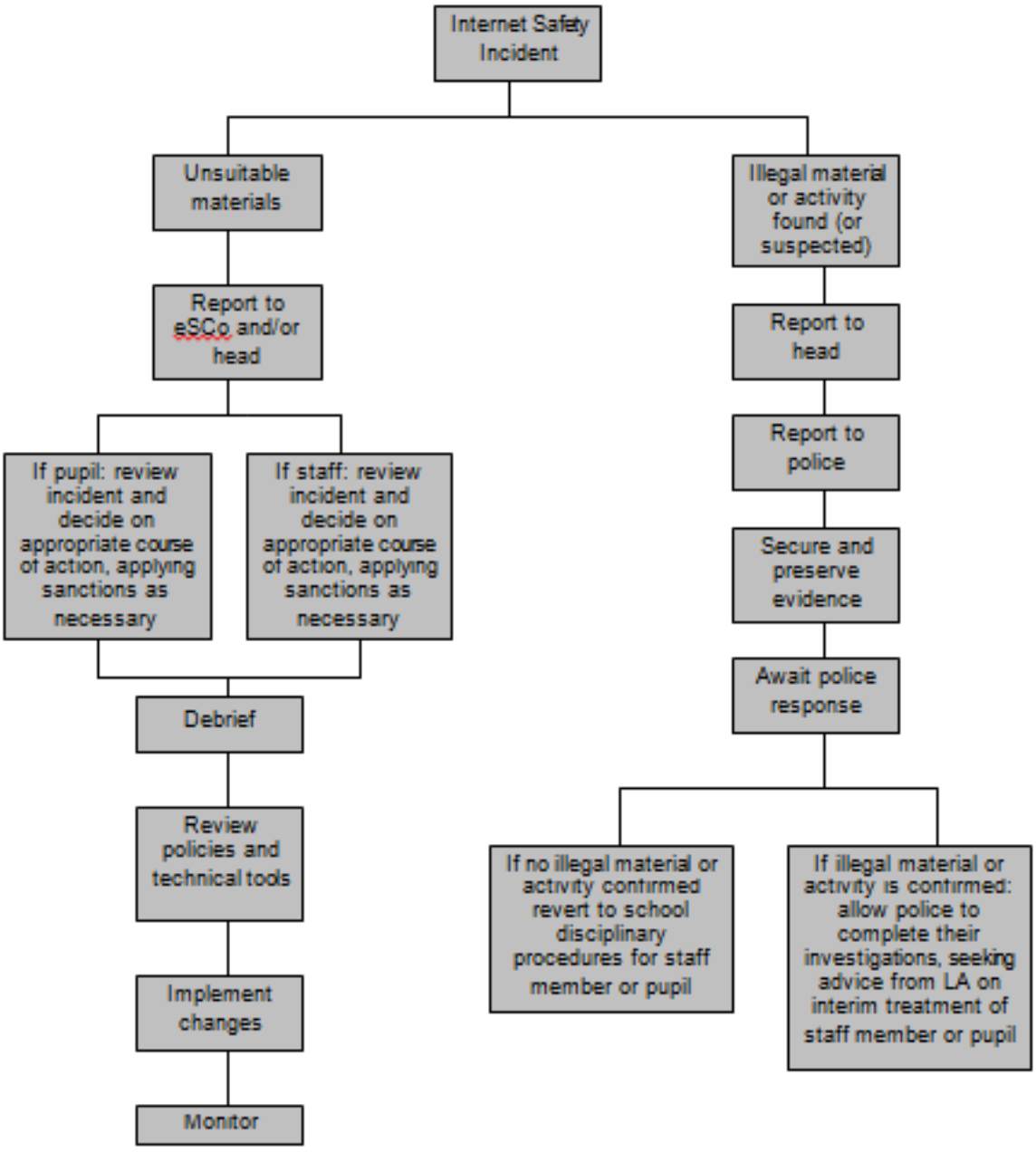
Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will receive regular e-safety training.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

Appendix A - Flowchart for responding to Internet safety incidents in school



Taken from Becta – E-safety 2005

Appendix B – E-safety rules for classrooms

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- All of our electronic communications (email, tweets, blog comments) are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We never save personal details such as our full name, address or date of birth on Evernote or Google Drive.
- We do not share files with people we do not know.

Appendix C

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's E-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that no personal devices (e.g. iPhone, personal iPad) will be used to take images or store data regarding pupils.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Folders containing information about pupils should be password protected on devices that are taken off school premises.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school eSafety Coordinator or the Designated Senior Person.
- I will ensure that any electronic communication with pupils is done through the class blog. All emails from pupils are forwarded to the e-safety co-ordinator and head of school.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ……..... Date: …….....

The following is part of the school's ICT policy relating to the use of all ICT equipment in school. Please read it carefully as breaches of this policy will be regarded as a serious matter.

Acceptable Use Statement

The computer system is owned by the school. "The computer system" means all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand-alone, or taken offsite.

Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences; or allow adults to enhance their own professional development. The school recognises that technologies such as the Internet and e-mail will have a profound effect on children's education and staff professional development in the coming years and the school's Internet Access Policy has been drawn up accordingly.

The installation of software or hardware unauthorised by the school, whether legitimately licensed or not is expressly forbidden.

The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.

All members of staff, students on placement, supply teachers etc must sign a copy of this policy statement before a system login password is granted. All children must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of Internet use.

Internet Access Policy Statement

All Internet activity should be appropriate to staff professional activities or the children's education;

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;
- The Internet may be accessed by staff and children throughout their hours in school;
- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media;
- Use of the school's Internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded;
- Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the school's network is the property of the school and making unauthorised copies of materials contained thereon maybe in breach of the Data Protection Act, Individual Copyright or Intellectual Property Rights;

- Use of materials stored on the school's network for personal financial gain is excluded;
- Posting anonymous messages and forwarding chain letters is excluded;
- The use of the Internet, e-mail, or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden;
- All web activity is monitored, including the content of e-mail, therefore it is the responsibility of the user to ensure that they have logged off the system when they have completed their task;
- Children must not be given unsupervised access to the Internet. For the purposes of this policy, "supervised" means that the user is within direct sight of a responsible adult;
- The teaching of Internet safety is included in the school's ICT Scheme of Work, but all teachers within all year groups should be including Internet safety issues as part of their discussions on the responsible use of the school's computer systems;
- All children must understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff.

Internet and System Monitoring

Through the LGfL internet activity is monitored by the system. It is the responsibility of the Administrator to review this activity periodically. It is the duty of the Administrator to report any transgressions of the school's Internet policy and/or use of obscene, racist or threatening language detected by the system to the New Technologies Team Leader and/or the Headteacher. Occasionally, it may be necessary for the Administrator to investigate attempted access to blocked sites, and in order to do this, the Administrator will need to set his/her Internet access rights to "Unrestricted". Whenever this happens, this should be recorded in the ICT violations register, and the Headteacher notified.

All serious transgressions of the school's Internet Access Policy are recorded in the school's ICT violations register. The violations register can be found in the Team Leader's folder.

Transgressions of Internet Policy and use of inappropriate language can be dealt with in a range of ways, including removal of Internet access rights; computer system access rights; meetings with parents or even exclusion; in accordance with the severity of the offence and the school's Behaviour Policy.

Breaches of Internet Access Policy by staff will be reported to the Headteacher and will be dealt with according to the school's and LA's disciplinary policy, or through prosecution by law.

Internet Publishing Statement

The school wishes the school's web site to reflect the diversity of activities, individuals and education that can be found at Rosendale Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles should be borne in mind:

- No video recording may be published without the written consent of the parents/legal guardian of the child concerned, and the child's own verbal consent; (See pro forma)

- Surnames of children should not be published, especially in conjunction with photographic or video material;

- No link should be made between an individual and any home address (including simply street names);

- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.

Use of Portable Equipment

The school provides portable ICT equipment such as laptop computers, colour printers and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

Exactly the same principles of acceptable use apply as in the Acceptable Use Statement above.

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from the use of a laptop computer and access should be negotiated with the individual concerned. Any difficulties should be referred to the New Technologies Team Leader;

- Certain equipment will remain in the care of the New Technologies Team Leader, and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the resource area;

- Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the Acceptable Use Statement and Internet Access Policy and that the equipment is fully insured from the moment it leaves the school premises.

- Any costs generated by the user at home, such as phone bills, printer cartridge etc. are the responsibility of the user;

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any portable equipment in their care to be returned for school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it;

- If an individual leaves the employment of the school, any equipment must be returned;

- Staff may install software on laptops to connect to the Internet from home. If in doubt seek advice;

- No other software, whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software;

- All staff are encouraged to make use of the school's anti-virus software for installation on any computers at home that they routinely use for school work.

Social media

Staff must not update personal social media accounts such as Facebook and Instagram during working hours.

Staff must not post photos of school or write anything about their jobs on personal social media accounts, i.e. Facebook. This includes “checking in”, photos of the school or equipment at school and status updates about your job or how you feel about any aspect of your job.

Staff must not post photos showing pupils onto personal social accounts.

Public social media accounts that are linked to school and your professional persona - i.e. Twitter, may be used to share about your job and may be updated during working hours and if the post is work related and includes @rosendaleschool.

Staff are advised not to be friends with parents of children at Rosendale on social media. If you are, it is your duty to alert colleagues you are also friends with.

I confirm I have read and understood the above statement.

Signed: ..... Date: .....

Name: .....

Institution: Rosendale Primary School