Rimrose Hope CE Primary School

E-Safety Policy

Rimrose Hope CE Primary School Online Safety

(E-Safety) Policy

1. Role of the E-safety leader

- Serve as a single point of contact for Sefton LSCB, school staff, governors, parents and pupils.
- The E-safety leader has a role within the SLT and is involved within the whole safeguarding process as roles may overlap.
- Maintain and drive forward the creation of an E-safety policy and Acceptable Use Policies (AUPs)
- Take responsibility for reviewing the policies and AUPs and relevant procedures at least annually and sooner in response to new technologies being used /analysis of logs and emerging trends.
- Make appropriate responses to policy breaches and ensure correct execution of reporting procedures including escalating incidents with external agencies as appropriate.
- Maintain logs for E-safety incidents and training provided to staff.
- Take responsibility for providing or arranging staff training as appropriate. Above all, staff should be made aware that they have professional responsibilities for pupils' safety in this area.
- Ensure that an E-safety education programme for children using technologies is in place.
- Create parent awareness of E-safety including updates on the school website.

Current pupil / staff access to the computers

• ICT Suite
• Multiple work stations located in the classrooms and corridors
• Staff room
• Head teacher office
• Main Office
• Laptops (Hall / SEN / Meeting Room / Reception)
• Mobile notebooks
• Personal equipment including Laptops / notebooks / mobile phones (inc. Smart Phones)

Internet access is connected through a System Wired Network and Wireless Network

E-Safety in the curriculum

ICT and online resources are increasingly used across the curriculum.

We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. e-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

• The school provides opportunities within a range of curriculum areas to teach about E-Safety

• Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum

• Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

• Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities

• Pupils are aware of the impact of Cyber bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

E-Safety skills development for staff

• Our staff receive regular information and training on eSafety and safeguarding issues in the form of inset and links through the eSafety lead.
• Details of the ongoing staff training programme can be found on the inset timetable.
• New staff receive information on the school's acceptable use policy as part of their induction.
• All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in

the event of misuse of technology by any member of the school community (see enclosed incident response form)
• All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Managing E-Safety messages

• E-safety posters will be prominently displayed
• We endeavour to embed e-safety messages across the curriculum whenever the internet and /or related technologies are used
• The e-safety policy will be introduced to the pupils and staff at the start of each school year

Information System Security

Our ISP is provided through Sefton School ICT Support. Sefton have a Service Level Agreement with Agilys. Amongst many services, the SLA provides the school with a Firewall (Smoothwall) to ensure the security of the network and to minimise all external threats. The firewall cluster is fully managed and monitored for denial of service and attack prevention A centralised URL (internet page content) filtering architecture is in place to manage, monitor and report on internet transactions. This platform allows for access to websites to be blocked based on subject of content request, individual website request or web functionality (i.e. image searching). This is an important feature to protect children and pupils from inappropriate internet content.

E-mails

Pupils have no access to an internal email account in the school. Accounts are however held by staff within the school and used on a regular basis. Staff are also able to access their personal email accounts from the school premises. Pupils are at present forbidden to email from school.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

Publishing pupil's images and work

Pupils' full names will not be used, unless authorised, anywhere on the Web site, particularly in association with photographs.

Permission from parents or carers will be obtained before photographs and or videos of pupils are published on the school Web site. This is done through a generic authorisation form, completed by parents.

Social networking and personal publishing

- The school will block, filter and forbid access to social networking sites.
- Newsgroups will be blocked 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 and parents will be advised that the use of social network spaces outside school is inappropriate for primary school children.
- In order to be eligible to sign up for Facebook, Bebo and MySpace, Snapchat, Twitter, users must be thirteen (13) years of age or older.

Protecting personal data

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

Authorising Internet access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The e - safety leader will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Assessing Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will

never appear on a school computer. Rimrose cannot accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- 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.

Introducing the e-safety policy to pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored.

Staff and the e-safety policy

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.

Enlisting parents' support

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

Acceptable User Policy

- Acceptable use policies (AUPs) agreements should be promoted amongst staff and parents and pupils.
- It will be necessary to have separate AUPs for staff and pupils.

- The AUP should cover the use of all technologies used.
- The AUP must be appropriate to the age of the reader and written in language that the user will understand.
- Pupils (and /or) their designated carers should be required to sign the AUP.
- The AUP should be reviewed regularly (at least every 12 months) and updated in line with developments in new technologies.
- The AUP should clearly define what uses of the technology are acceptable (and those that are not.)
- Sanctions for not complying with the AUP should be stated
- The AUP should state what monitoring and reporting of individual usage is in place.

Acceptable Use Agreement / E-Safety Rules

✓ I will only use ICT in school for school purposes.

✓ I will not tell other people my ICT passwords.

✓ I will only open/delete my own files.

✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

✓ 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 unless this is part of a school project approved by my teacher and a responsible adult comes with me.

✓ I will be responsible for my behaviour when using ICT 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. I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-Safety

Dear Parent/ Carer,

ICT including the internet, email 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 ICT.

Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page.

If you have any concerns or would like some explanation please contact Mr. Crilly

Parent/ carer signature

We have discussed this and ……..(child name) agrees to follow the E-Safety rules and to support the safe use of ICT at Rimrose Hope Church of England Primary School. Parent/ Carer Signature
…… Class …… Date ……

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life at Rimrose Hope. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Miss A Sullivan school e-safety coordinator.

➢ 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 Head 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 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 email address, to pupils.

➢ I will only use a secure email system(s) for any school business.

➢ I will ensure that personal data (such as data held on SIMS and Target Tracker) 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 Assistant Heads, Head or Governing Body.

➢ I will not install any hardware or software without the permission of Miss Anna Sullivan

➢ 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 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 without the permission of the parent/ carer, member of staff or Head teacher.

➢ 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 line manager or Head Teacher.

➢ 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 ensure that I gain permission before posting reference to or images of any member of staff on any social networking site such as Facebook or Twitter...

➢ I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT.

User Signature

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

Signature …… Date ……

Full Name ……(printed) Job title . . . . . .

Breach of Policy / AUP

Sanctions Pupils:

Pupils found to be wilfully breaking their acceptable use agreements will be dealt with by the class teacher. Severe breaches including cyber bullying and downloading of offensive material will be dealt with by the SLT. Sanctions will fall in line with equivalent offences found in the behaviour policy. Persistent low-level breeches may include the banning of the use of ICT during school time for a set term.

Breeches by adults and staff may be lead to disciplinary action and will be dealt with by the Head teacher and or Governors.

Incident Log Details of incidents should be recorded by the e-safety Lead on our Cpoms system.

Incidents should then be forwarded to the Head teacher.

Date & Time

Name of pupil

Details

Incidents that involve a direct safeguarding threat to pupils or staff must be referred immediately to a senior member of staff.

The action then will fall in line with the Incident Response Form as produced by Sefton Local Safeguarding Children Board.

Appendix 4 Relevant Paragraphs from the school safeguarding policy.

Mobile phones and cameras

Staff are allowed to bring their personal phones to school for their own use but will limit such use to non-contact time when pupils are not present. Staff members' personal phones will remain in their bags or cupboards during contact time with pupils.

Staff will not take pictures or recordings of pupils on their personal phones or cameras.

As a school we follow the General Data Protection Regulation and Data Protection Act 2018 when taking and storing photos and recordings for use in the school, all photographs are taken using school Ipads/camera devices. Images are uploaded and stored onto a school based cloud called Earwig. Only photographs of children with parental consent will be displayed publicly (school website, Twitter, Earwig- Parent View).

To protect pupils we will:

- seek their consent on enrolment for photographs to be taken or published (for example, on our website or in newspapers or publications);
- seek parental consent;
- use only the pupil's first name with an image;
- ensure pupils are appropriately dressed; and
- encourage pupils to tell us if they are worried about any photographs that are taken of them.

Children are not prohibited to bring mobile/camera devices to school; however, in the event of a child having a mobile device on them (by a letter of request by parents for safeguarding purposes e.g. walking home alone) the device will be stored and locked away in the office and the children can retrieve the device at the end of the day.

Online Safety

Children and young people commonly use electronic equipment including mobile phones, tablets and computers on a daily basis to access the internet and share content and images via social networking sites such as Facebook, Twitter, MSN, Tumblr, Snapchat and Instagram.

Those technologies and the internet are a source of fun, entertainment, communication and education. Unfortunately, however, some adults and young people will use those technologies to harm children. That harm might range from sending hurtful or abusive texts and emails to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings. Pupils may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity.

Chat rooms and social networking sites are the more obvious sources of inappropriate and harmful behaviour and pupils are not allowed to access those sites in school. Chat rooms and social networking sites are the more obvious sources of inappropriate and harmful behaviour and pupils are not allowed to access those sites in school. Many pupils own or have access to hand held devices and parents are encouraged to consider measures to keep their children safe when using the internet and social media at home and in the community. (E safety policy can be found on the school's website). No access is given within school to inappropriate sites – either on our network or through own devices (as they are not permitted to be used on site and cannot access our internet). Appropriate filters and monitoring systems that are not too restrictive as to restrict a child's education; are in place as referred in *Keeping Children Safe in Education 2018* (Annex C). The school's **online safety policy** can be accessed from the staffroom and school website and explains how we try to keep pupils safe in school and protect and educate pupils in the safe use of technology. Cyberbullying and sexting by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. Serious incidents may be managed in line with our sexual exploitation policy or child protection procedures (see 'Sexting' below). All staff receive online safety training and the school's e-safety coordinator is L A Crilly.

Gaming

Online gaming is an activity that the majority of children and many adults get involved in.

The school will raise awareness by:

- Talking to parents and carers about the games their children play and help them identify whether they are appropriate.
- Supporting parents in identifying the most effective way of safeguarding their children by using parental controls and child safety mode.
- Talking to parents about setting boundaries and time limits when games are played.
- Highlighting relevant resources.
- Making our children aware of the dangers including of grooming and how to keep themselves safe
- Making our children aware of how to report concerns

Staff/pupil relationships

Staff also receive advice regarding personal online activity, use of social networking and electronic communication with pupils, about which there are strict rules highlighted in the Code of Conduct. Staff found to be in breach of these rules may the subject of a referral to the Designated Officer in the Local Authority and may be subject to disciplinary action

Cyber-bullying

Central to our School's anti-bullying policy is the principle that '*bullying is always unacceptable*' and that '*all pupils have a right not to be bullied*'.

The school recognises that it must take note of bullying perpetrated outside school which spills over into the school and so we will respond to any cyber-

bullying we become aware of carried out by pupils when they are away from the site.

Cyber-bullying is defined as "an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself."

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in on-line forums

Cyber-bullying may be at a level where it is criminal.

If we become aware of any incidents of cyber-bullying, we will consider each case individually as to any criminal act that may have been committed. The school will pass on information to the police if it feels that it is appropriate or are required to do so. As a school, we encourage children to report any bullying incidents on our website using our 'Tell Rimzo' and 'Whisper' applications.

Bullying

While bullying between children is not a separate category of abuse and neglect, it is a very serious issue that can cause considerable anxiety and distress. At its most serious level, bullying can have a disastrous effect on a child's well-being and in very rare cases has been a feature in the suicide of some young people.

All incidences of bullying, including cyber-bullying and prejudice-based bullying should be reported and will be managed through our anti-bullying procedures. All pupils and parents receive a copy of the procedures on joining the school and the subject of bullying is addressed at regular intervals in PSHE education.

If the bullying is particularly serious, or the anti-bullying procedures are deemed to be ineffective, the Headteacher and the DSL will consider implementing early help) or child protection procedures.

Please also refer to issues in relation to children who are sexually harmful or abusive towards other children below.

Peer on Peer Abuse

All staff should be aware that safeguarding issues can manifest themselves via peer on peer abuse. This is most likely to include, but may not be limited to:

- bullying (including cyber bullying)
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm
- sexual violence and sexual harassment
- sexting (also known as youth produced sexual imagery); and
- initiation/hazing type violence and rituals

Managing Allegations against other Pupils (peer on peer abuse)

We believe that all children have a right to attend school and learn in a safe environment. Children should be free from harm by adults in the school and other pupils. We recognise that some pupils will sometimes negatively affect the learning and wellbeing of others and their behaviour will generally be dealt with under the School's Whole School Behaviour Policy. It is not enough to respond to incidents as they arise and we strive to create an environment that actively discourages abuse and challenges the attitudes which underlie it. The school has a Policy which includes bullying, and sexual and racial harassment.

All staff are made aware that safeguarding issues can manifest themselves via peer on peer abuse. This is most likely to include, but not limited to: bullying (including cyber bullying), gender-based violence/sexual assaults and sexting.

Sexting

As with all other actual or possible safeguarding issues and concerns, staff should not make their own judgements about whether a 'sexting' issue is more or less serious enough to warrant a report to the DSL. What may seem like less serious concerns to individual members of staff may be more significant when considered in the light of other information known to the DSL, which the member of staff may not be aware of.

If staff become concerned about a 'sexting' issue in relation to a device in the possession of a student (e.g. mobile phone, tablet, digital camera), the member of staff should secure the device (i.e. it should be confiscated). This is consistent with DfE advice **Searching, Screening and Confiscation - Advice for Headteachers, school staff and governing bodies (DfE February 2014- updated 2018)**, page 11 'After the search'.

The confiscated device will be passed immediately to the DSL. Staff will not look at or print any indecent images.

The DSL will make a judgement about whether the reported 'sexting' incident is experimental as in section 12 above or aggravated.

Aggravated incidents involve criminal or abusive elements beyond the creation, sending or possession of sexual images created by young people. These include possible adult involvement or criminal or abusive behaviour by young people such as sexual abuse, extortion, threats, malicious conduct arising from personal conflicts, or creation or sending or showing of images without the knowledge or against the will of a young person who is pictured.

Aggravated incidents of sexting will usually be referred to Sefton's Multi-Agency Safeguarding Hub (MASH) for advice about whether or not a response by the Police and/or Children's Social Care is required. This will facilitate consideration of whether:

- there are any offences that warrant a Police investigation;
- child protection procedures need to be invoked;
- parents/carers require support in order to safeguard their children ;
- a multi-agency sexual exploitation (MASE) meeting is required;

- any of the perpetrators and/or victims require additional support. This may require the initiation of a TAF and the offer of Early Help services.

Examples of aggravated incidents include:

 any evidence of pressurising, intimidating, bullying, extortion and/or threatening of students by one or more other students to create and share indecent images of themselves;

- pressure applied to a number of students (e.g. all female students in a class or year group) to create and share indecent images of themselves;
- pressurising a younger student or students to create and share indecent images of themselves;
- pressurising a student with additional vulnerability to create and share indecent images of themselves;
- dissemination of indecent images of young people to a significant number of others (either as an act of so-called 'revenge porn' or exploitation);
- any evidence of adult involvement in acquiring, creating or disseminating indecent images of young people (possibly by an adult pretending to be a young person known to the victim).

The DSL will make a judgement about whether or not a situation in which indecent images have been shared with a small number of others in a known friendship group with no previous concerns constitutes an aggravated incident; or whether the school is able to contain the situation in partnership with all parents of the students involved, arrange for the parents to ensure that all indecent images are deleted and that the young people involved learn from the incident in order to keep themselves safe in future.

In the latter instance, the DSL will usually consult with the Police and/or Children's Social Care through the MASH to check that no other relevant information is held by those agencies and to ensure an agreed response is documented before proceeding.