Rosemount Primary and Nursery School E Safety Policy

Rosemount Primary and Nursery School

E-Safety Policy
And
Acceptable Use Agreement

Introduction

Our vision in Rosemount Primary and Nursery School is one where each child and staff member feels valued, respected and loved; where talents and abilities are nurtured to enable all to reach their potential, in an inclusive environment committed to our shared Christian values.

Our school is committed to providing a safe, positive, inclusive and respectful learning environment for all members of the school community. We also have a responsibility to contribute, in whatever way we can, to the protecting and maintaining such an environment.

In Rosemount Primary and Nursery School we understand our responsibility to educate our pupils on e-safety issues. E-safety is short for 'electronic safety' and encompasses not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. We aim to teach children appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- iPads and other tablet devices with Internet access

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, our staff, pupils and parents need to be aware of the range of risks associated with the use of internet technologies.

The Internet

The internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the internet is an essential skill for children as they grow up in the modern world. The internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings our pupils into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable.

Key concerns are:

1. Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons.
Children should be taught:

- That people are not always who they say they are
- That "Stranger Danger" applies to the people they encounter through the internet
- That they should never give out personal details
- That they should never meet alone anyone contacted via the internet
- That once they publish information e.g. send inappropriate photograph, it can be easily shared.

2. Inappropriate Content

Through the internet there are unsuitable materials in many varieties. Anyone can post material on the internet.
Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content.
Materials may express extreme views e.g. some use the web to publish information on weapons, crime and racism, which would be, restricted elsewhere.
Materials may contain misleading and inaccurate information e.g. some use the web to promote activities which are harmful such as bullying.
Children should be taught:

- That information on the internet is not always accurate or true.
- To question the source of information How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

(see Appendix 1 – SMART Tips)

Excessive Commercialism

The internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising, which is very persuasive.
Children should be taught:

- Not to fill out forms with personal details
- Not to use an adult's credit card number to order online products

If children are to use the internet in places other than at school e.g. libraries, clubs or at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to all problems of internet safety. Teachers, pupils and parents must be vigilant.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT co-ordinator, to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and any relevant training. The ICT co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.

It is the role of the Principal/ICT Co-ordinator to update senior management and governors with regard to e-safety so they all have an understanding of e-safety in relation to local and national guidelines and advice.

Writing and Reviewing the E-Safety Policy

This policy, supported by the school's Acceptable Use Agreement, is there to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Positive Behaviour, Child Protection and Anti-Bullying.

This policy has been agreed by the staff and approved by the Board of Governors. The E-Safety Policy and its implementation will be reviewed annually or in the light of any new legislation or guidance.

E-Safety Skills' Development for Staff

- All staff receive information and are updated regularly on e-safety issues by the ICT co-ordinator at staff meetings or via feedback from the ICT Development Team.
- All staff have been made aware of their 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.
- New staff members receive information on the school's Acceptable Use Agreement and Staff Code of Conduct as part of their induction.
- All staff are encouraged to incorporate e-safety activities and awareness within their lessons.

E-Safety Information for Parents/Guardians

 Parents/guardians are asked to read through and sign the Acceptable Use Agreement on behalf of their child following P1 Induction or when a new child starts school (see Appendix 3).

- Parents/guardians are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school website contains a link to CEOP's thinkuknow.
- The school will communicate relevant e-safety information through letters, newsletters and the school website.

Parents should remember that it is important to promote e-safety at home and to monitor internet use. Some recommended advice includes:

- Talk to your children about the benefits and dangers of the internet so as empowering them to use it safely
- Keep the computer in a communal area at home
- Be aware that children have access to the internet via gaming stations and portable technologies such as tablets, iPads, smart phones and watches
- Monitor on-line time and be aware of excessive hours spent on the internet
- Take an interest in what your children are doing online. Discuss with the children what they are seeing and using on the internet
- Advise children to take care and to use the Internet in a sensible and responsible manner
- Know the SMART tips that the children learn in school (see Appendix 1)
- Discuss the fact that there are websites/social networking activities which are unsuitable
- Discuss how children should respond to unsuitable materials or requests
- Remind children never to give out personal information online
- Remind children that people online may not be who they say they are
- Be vigilant. Ensure that children do not arrange to meet someone they have been in contact with online
- Be aware that children may be using the internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Teaching and Learning

Internet Use

- Teachers will plan and provide opportunities within a range of curriculum areas to teach e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. 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/guardian, teacher/trusted member of staff or an organisation such as Childline/CEOP.
- The school internet access is filtered through the C2k managed service.
- No filtering service is 100% effective; therefore all children's use of the internet is with the permission of an adult.

- Use of the internet is a planned activity. Aimless surfing is not allowed. Children are taught to use the internet in response to a need e.g. a question which has arisen from work in class.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Children are taught to be 'Internet Wise'. Children are made aware of the Rules for Responsible Network and Internet Use (see Appendix 2) which are displayed in their classroom.
- Children are encouraged to discuss what to do if they come across inappropriate material.
- Teachers will avail of opportunities to promote e-safety when appropriate e.g. C2K Newsdesk, school assemblies, e-safety competitions, Internet Safety Day, Cyber Bullying within Anti-Bullying context etc.

Children are taught:

Being online and using the internet is just like being in the real world – you can chat to people, play games and share pictures. But sometimes things happen which can make you upset. People may say nasty things to you which upset you, or you may see something that you don't like. If this happens, you must remember that it's not your fault.

☆ Always tell a trusted adult straight away if you are upset or worried about something that has happened online.

☆ Remember to SAVE any messages that have upset you so you can show them to the person you tell – they will be able to help you.

☆ If you don't want to talk to a trusted adult, there are trained counsellors who can listen and advise at Childline. You can call this number for free 08001111.

Multimedia Technology

In Rosemount Primary and Nursery School we are aware of the educational benefits that proper use of communication technology provides for our pupils and we advocate this in order to promote and enhance the learning experiences for our pupils. We are delighted to have iPads available for pupil use, however we are also very aware of the potential for hurt and harm to individuals if this technology is misused and abused. Consequently, the school wants to make the provision safe for use by pupils so pupils are not permitted to use iPads for the following:

- to send inappropriate pictures/photos

- to send hurtful messages

- to access social networking sites e.g. Facebook, Snapchat, Instagram etc

- to use bad language

- to take photos or videos of pupils/teachers without permission or direction from the teacher.

NB. Deliberate access to inappropriate materials or breaking of internet rules by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the E-Safety Incident Logbook. The school principal and ICT co-ordinator will agree appropriate sanctions e.g. a pupil's internet maybe access disabled. When this is the case, parents/guardians will be informed and further consequences maybe necessary depending on the level of severity of the incident.

Social Networking

- The school C2k system will block access to social networking sites to pupils.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils; the legal requirement for most sites is 13 years.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals when they are at an age to be on social networking sites.
- Our pupils are asked to report any incidents of cyber bullying to the school.
- School staff will not add children as 'friends' if they use social networking sites.

Mobile Technologies

- Pupils are not allowed personal mobile phones, smart watches, tablets, iPads etc in school.
- Staff are not permitted to use personal mobile phones at any stage when pupils are present, unless permission has been given by the principal e.g. on a school trip.

Managing Video- Conferencing

- Videoconferencing will be via the C2k network using Collaberate, to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Publishing Pupils' Images and Work

- Written permission from parents/guardians will be obtained following P1 Induction, or when a newcomer pupil starts school, before photographs of pupils are published on the school website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/guardians may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs on the school website.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents/guardians.

Policy Decisions

Authorising Internet Access

- Pupil instruction in responsible and safe use should precede any internet access and all children should be taught to abide by the school's E-Safety rules. These 'Rules for Responsible Network and Internet Use' are displayed clearly in ICT suite.
- Access to the internet will be supervised. Pupils are not permitted to be on the internet during break/lunch time unless supervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils following P1 induction or when a newcomer pupil starts, giving consent for their child to use the internet in school following the school's rules and within the constraints detailed in the school's E-Safety Policy. Any parent/guardian who may wish for their child to 'opt out' from using the internet may do so by putting this in writing to the school.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff (see Appendix 4) before using any school ICT resource.
- Each user is provided with internet filtering via the C2K Education Network solution. The C2K network has internet filtering based on a websense filtering solution whereby categories of sites can be made available to users, while access to other areas will be restricted.
- The filtering system categorises all websites as either red (unavailable) or green (available). By default, all users are given access to a core set of green sites.

School choice:

In addition to the default sites the school can choose to make users members of one or more internet-related security groups. These are:

- Social Networking
- Streaming Media
- Internet Advanced

Internet access for senior management, teachers, assistants, office staff etc is allocated in accordance to their roles and responsibilities. The final decision for allocation of access lies with the school principal and the Board of Governors.

Note: *The same C2k filtering applies across the C2k network, whether using a C2k core desktop computer, a notebook or an iPad. This consistency is essential to ensure the safety and integrity of C2k's internet provision.*

Password Security

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details are never shared with pupils.
- All pupils in KS1 and KS2 are provided with an individual login username and password. Children in Foundation Stage have a 'simplified' login set.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Handling E-Safety Complaints

- Complaints of internet misuse or breaking internet safety rules will be dealt with by the principal or a senior member of staff.
- Deliberate access to inappropriate materials or breaking of internet safety rules by any user will lead to the incident being logged by the Principal/ICT Co-ordinator and recorded in the E-Safety Incident Logbook. Appropriate sanctions will be agreed by the school principal and ICT co-ordinator e.g. pupils internet access disabled. When this is the case, parents/guardians will be informed and further consequences maybe necessary depending on the level of severity of the incident.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with the school's Safeguarding Policy and Procedures.

Communicating the Policy

Pupils

- Rules for Responsible Network and Internet Safety and SMART tips are displayed in ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week etc.
- Pupils will be informed that network and internet use will be monitored.

Staff

- All staff have a copy of the school's E-Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff need to be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop/iPad/portable device issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to internet access, data protection and use of software. School laptops, ipads and portable devices are not permitted to be taken from school, unless with prior agreement with the principal.
- All staff must sign up to the Acceptable Use Agreement.

Parents

- Parents are sent a copy of the E-Safety and Acceptable Use Policy when it is updated. Opportunity is made available for their input and comment.
- All parents/guardians are required to sign the Acceptable Use Agreement when their child starts Primary 1 or when a child starts Rosemount Primary and Nursery School after Primary 1.
- The E-Safety and Acceptable Use Policy is available on the school website to download.
- Parents are invited to any relevant workshops in school on the area of e-safety.
- Parents are kept informed of any recent advice from the Department of Education, updated websites and useful phone numbers (see Appendix 5) or relevant information that is shared with the school from outside organisations e.g. NSPCC.

Links to other Policies

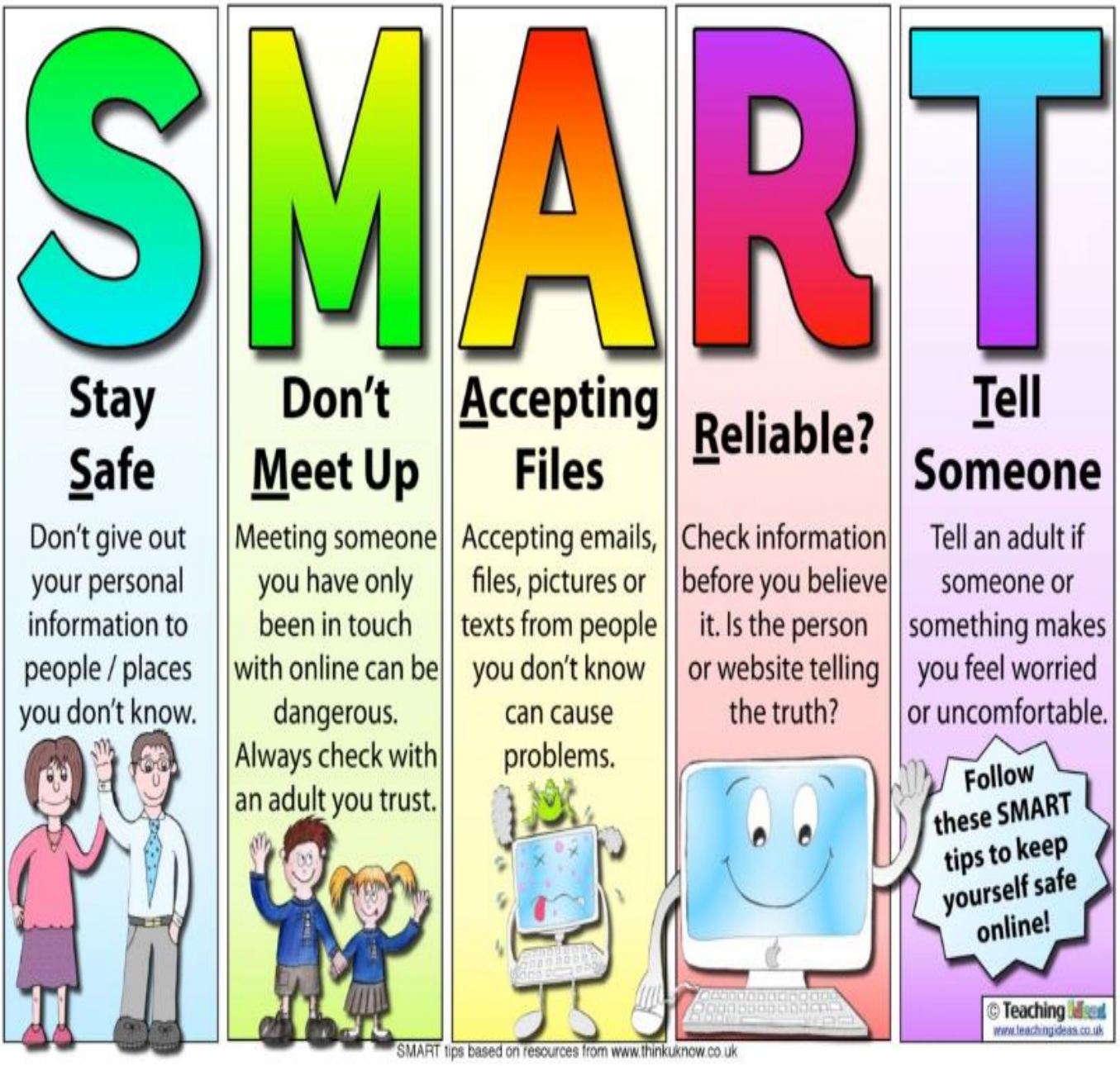
- ICT Policy
- Child Protection Policy
- Promoting Positive Behaviour Policy
- Anti-Bullying Policy

Monitoring and review:

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT co-ordinator.
This policy will be reviewed on an annual basis or when further guidance/ legislation makes it necessary.

APPENDIX 1

SMART Tips



APPENDIX 2

Rosemount Primary and Nursery School

Rules for Responsible Network and Internet Use

In school we have a computer network with internet access to help our learning. These rules will help keep us safe and help us be fair to others.

- Using the network:
- I will only access the network with the login and password I have been issued. I will keep my username and password private
- I will not access other people's area or files
- I will not download anything onto the school computer.

- Using the Internet:
- I will ask permission from a teacher before using the internet
- I will only access the websites that my teacher has given to me
- I will use the internet for school purposes only
- I will never post an unsuitable image online
- I will not use a search engine such as Google etc unless I have gone through the route I want to take with my teacher and he/she has checked it for me
- If I see anything I am unhappy with or I know to be inappropriate I will report it to my teacher/member of staff immediately because this will help protect other pupils and myself
- I understand that the school may check my computer files and may monitor the internet sites I visit
- I will not give my full name, my home address or telephone number when on the internet
- I will not arrange to meet with anyone I have met over the internet.

APPENDIX 3

Rosemount Primary and Nursery School

Principal: Mr P. Bradley

Tel: 02871265605
e-mail:
www.rosemount.com

Appendix 4 Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of 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 Mr P Bradley, Principal or ICT coordinator, Mrs J. Devlin.

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 Principal or Board of Governors.

- 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 e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) 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 Principal or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of C2k.
- 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 Principal.
- 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 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 Principal.
- 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 e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

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 . . . . . .

Appendix 5

Useful Phone Numbers and Websites

- Childline 08001111

- Police 101

- Lifeline 0808808

- www.thinkuknow.co.uk

- www.bbc.co.uk/cbbc/curations/stay-safe

- www.getsafeonline.org

- www.safetynetkids.org.uk/personal-safety/staying-safe-online

- www.kidsmart.org.uk

- www.saferinternet.org.uk

- www.nspcc.org.uk>preventing abuse>keeping children safe

- www.childnet.com

- www.deni.gov.uk/index/pupils-and-parents/pupils.htm