

Rosetta Primary School



Policy on Acceptable use of
the Internet and Digital
technologies and E-Safety

February 2018

Updated December 2020

Acceptable Use of The Internet and Digital Technologies Policy

Introduction

In Rosetta we recognise that the internet and other digital technologies are very powerful resources, which can enhance and potentially transform teaching and learning when used effectively and appropriately. The internet is an essential element of 21st century life for education, business and social interaction. Rosetta Primary School provides pupils with opportunities to use the excellent resources on the internet, along with the developing skills necessary to access, analyse and evaluate them. This includes educating our children about the potential dangers found on the internet, and our e-Safety Policy further explains our role in protecting our pupils.

Code of Practice for Safe and Effective Use

When using the internet, email systems and digital technologies, all users must comply with relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. The Code of Practice for Rosetta Primary School sets out for all users, staff and pupils, what is safe and acceptable and what is not.

The scope of the Code of Practice covers fixed and mobile internet, school desktop computers, laptops, iPads and digital video equipment. It should be noted that the use of devices owned personally by staff and pupils but brought onto school premises or taken on trips (e.g. mobile phones, camera phones, iPads etc.) is subject to the same requirements as technology provided by the school.

The ICT Co-ordinator will monitor the effectiveness of the Code of Practice, particularly in light of new developments in technology.

Code of Practice for Pupils

Pupil access to the internet is through a filtered service provided by C2k, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

In addition, the following measures have been adopted by Rosetta Primary School to ensure our pupils do not access any inappropriate material:

- Our e-Safety rules and advice for staying 'SMART' online are delivered to pupils and displayed prominently in the ICT Room/classrooms;
- Pupils using the internet will normally be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and is supervised, where possible;
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group, unless engaging in independent research activities;
- Pupils are not permitted to download apps onto school iPads;
- Pupils are educated in the safe and effective use of the internet, through a progressive scheme of lessons;

- The use of mobile phones by pupils is not permitted on the school premises during school hours;
- Pupil access to social networking sites is blocked by the C2k filters so pupils do not have access to them in the school environment. During school hours, pupils are forbidden to play computer games unless specifically assigned by the teacher.

Code of Practice for staff

Staff have agreed to the following Code of Safe Practice:

- All staff will be given the School E-Safety Policy and its application and importance explained.
- All staff will receive regular information and training on E-Safety issues through the Co-ordinator/ICT Team at staff meetings.
- Pupils accessing the internet should ideally be supervised by an adult at all times.
- All pupils are aware of the rules for the safe and effective use of the Computers/iPads. These are displayed in the ICT Room and classrooms and should be discussed with pupils.
- Equipment, websites, apps and materials recommended for use of pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age-appropriate, especially if these have been downloaded from a non-C2k filtered network.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/ICT Co-ordinators.
- 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.
- New staff members will receive a copy of Acceptable Use of The Internet and Digital Technologies and E-Safety policy.
- All staff are encouraged to incorporate E-Safety into their activities and awareness within their lessons.
- In the interests of the system security staff passwords should only be shared with the network manager.
- Teachers are aware that the C2K system tracks all internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of pupils should, where possible, be taken with a school camera/ iPad and images will be stored on a centralised area on the school network, accessible only to teaching staff.
- School systems may not be used for unauthorised commercial transactions.
- Staff are not permitted to engage or use any social network or other internet forum in order to discuss any member of staff, pupil, parent or other school issue. This is connected to the school's Social Media Policy.

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2k can accept liability under such circumstances.

Internet Safety Awareness

In Rosetta Primary School we believe that, alongside having written policies on e-Safety Acceptable Use of the Internet & Digital Technologies and Social Media, it is essential to educate all users in the safe and effective use of the internet and other forms of digital communication.

We see education in appropriate, effective and safe use of the internet as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

Internet Safety Awareness for pupils

Rules for e-Safety and Using Computers/iPads are discussed with pupils and are prominently displayed in the ICT Room and classrooms. 'SMART' tips are also discussed with the children and displayed. The school takes part in Safer Internet Day annually with staff delivering e-Safety lessons, and visitors are brought in to run workshops with KS2 children where possible.

Internet Safety Awareness for Staff

The ICT Co-ordinators and Designated Teacher for Child Protection are kept informed and updated on issues relating to Internet Safety. This information is then disseminated to all teaching staff, classroom assistants and supervisory assistants on a regular basis. Advice is also available in the Fronter 'Safer Internet' Room.

Health and Safety

Rosetta Primary School has attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, in classrooms and the ICT Room. Pupils are supervised at all times when Interactive Whiteboards and digital projectors are being used.

Digital and Video Images of Pupils

Parental permission is sought to cover the use of photographs of pupils on the school website, in the local press and for displays etc. within school, and written permission must be obtained from a parent/carer.

School Website

The school's website address is www.rosettaps.co.uk. As our website and app continues to grow, we intend to develop the existing gallery/articles featuring both pupils' work and the pupils themselves engaged in a variety of noteworthy activities. When posting photographs to the site we will ensure that:

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Parents/carers 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 on the school website in association with photographs.
- Teachers will endeavour to take pictures of groups or group activities, however individual pictures will be used from time to time.
- Staff are allowed to take digital/video images to support educational purposes following the E-Safety policy. Images should be taken on school equipment, e.g. school cameras, iPads.
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.
- Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area on the school network, accessible only to teaching staff. Photographs of pupils are removed when they leave the school.

Social Networking

The school network system, provided by C2K will block access to social networking sites. Pupils and parents will be advised that the use of many social network pages outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.

- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils will be advised not to place personal photos on any social network space. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location e.g. house number, street name or school.
- Our pupils are asked to report any incidents of bullying to the school.
- Pupils will be advised that sending abusive messages or images in any online format will be considered as bullying and will be dealt with accordingly.

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. Due to the ever-changing nature of the internet and digital technologies, this policy and its effectiveness will be reviewed annually.

E-Safety Policy

Introduction

In Rosetta Primary School we are aware of our responsibility to educate pupils and provide them, and parents, with information relating to e-Safety. Our aim is to teach children about appropriate online behaviours, and to think carefully about various situations to help them remain safe and legal when using the internet and related technologies both in school and at home.

What is E-Safety?

- E-Safety is short for 'electronic safety'.
- It highlights the responsibility of the school, all staff, governors and parents to mitigate risk through reasonable planning and actions. e-Safety covers not only internet technologies but also electronic communications via other devices e.g mobile phones, games consoles and wireless technology.

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 phone with text, video and/or web functionality
- Internet connected TV
- Other mobile devices with web functionality.

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet Technologies.

In Rosetta Primary School we understand the responsibility to educate our pupils in E-Safety issues. We aim to teach the children appropriate behaviours and critical thinking to enable them to remain both safe and legal when using internet and related technologies, in and beyond the context of the classroom.

The school has a duty to provide pupils with quality internet access as part of their learning experience. The internet is part of the statutory curriculum and an entitlement for pupils as part of their learning experience. It is used in school to raise educational standards, promote pupil achievement and as a necessary tool for staff to support their professional work. The internet also enhances the school's management information and business administration systems.

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 young people 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:

Potential Contact

Children may come into contact with someone 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, and
- That once they publish information it can be disseminated with ease and cannot be destroyed.

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. Materials may express extreme views e.g. some use the web to publish information on weapons and crime, which would be restricted elsewhere. Materials may contain misleading and inaccurate information.

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.

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 a lot of personal details.
- Not to order products online or apps without first seeking permission from a parent/carer.

As children have access to the internet in a variety of places other than school it is important that we educate them in how to behave appropriately online, and to understand the importance of discussing problems and issues that might arise. It is also important that all staff, parents and carers must be vigilant when children are using the internet in school.

Cyber-bullying

Staff in Rosetta Primary School are aware that pupils may face conduct risks when online, either engaging in, or being the target of bullying behaviour in peer-to-peer exchanges, and/or are at risk of entrapment and/or blackmail. Cyber-bullying via electronic methods of communication may occur both in and out of school.

Social media is rarely used for learning and teaching within Rosetta Primary School, but we recognise it is important that our children are educated about the risks and issues related to social media. Each of

the social media technologies can offer much to schools and pupils, but each brings its own unique issues and concerns.

Cyber-bullying can take many different forms including:

- Email - nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms - potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites - typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming - abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones - examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information - may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for those engaging in bullying behaviour, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence.

To help children understand these four identified areas of risk, and to promote the importance of a positive digital footprint, e-Safety Rules and Rules for Using Computers/iPads will be displayed in all classrooms and the ICT Room, along with 'SMART' tips for staying safe online. These will be discussed with the pupils at the start of each year and reminders issued each term. Each class will engage in lessons related to Internet safety and as a whole school we participate in Safer Internet Day annually.

Pupils will also be informed that their C2k network and Internet use will be monitored.

E-Safety Information for Parents/Carers

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and/or used on the school website.
- The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web stay safe page.
- The school will communicate and promote relevant E-Safety information through newsletters and the school website.
- The school will communicate with and promote outside bodies such as NSPCC and the PSNI to ensure parents are kept up to date and informed of Internet information.
- Internet issues will be handled sensitively and parents will be advised accordingly.

Parents should remember that it is important to promote E-Safety in the home and to monitor internet

use.

- Keep the computer/iPad/tablet in a communal area of the home.
- Make use of parental controls/ filters on the internet and devices
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones/games consoles/tablets.
- Monitor on-line time and be aware of excessive hours spent on the internet.
- Take an interest in what children are doing. 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.
- 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 on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet online.
- Be aware that children maybe using the internet in places other than their own home or at school and that this internet use may not be filtered or supervised.

Teaching and Learning

Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety. Pupils will be taught SMART rules.
- Key E-Safety messages will be reinforced annually through an assembly and Safer Internet Day.
- The school will liaise with local organisations to establish a theme or common approach to E - Safety in the form of a workshop/talk. This may take place in Key stages or as a whole school approach.
- 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/carer, Safeguarding Team, Class Teacher/trusted member of staff.

Safety is a focus in all relevant areas of the curriculum.

- 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 should be supervised by an adult.

- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Where pupils are allowed to freely search the internet e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- 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.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.
- When using digital images, pupils are taught about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff act as good role models in their own use of ICT.

Communicating the Policy

Introducing the e-Safety Policy to pupils

- E-Safety rules will be displayed in all classrooms 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/Safer Internet Day.
- 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.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop/iPad 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/Apps, both in and out of school.

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 well-informed of current E-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and the Childnet.

The ICT Co-ordinator has responsibility for leading and monitoring the implementation of E- Safety throughout the school.

The Principal/ICT Co-ordinator have the responsibility to update the Senior Leadership Team and Governors with regard to E-Safety and all governors should have an understanding of the issues at our school in relation to local and national guidelines and advice.

Monitoring and review

This policy, supported by the school's Acceptable Use Agreement for staff and pupils, is to protect the interests and safety for the whole school community. It has been agreed by the Senior Leadership Team, Staff and approved by the Governing Body. The E-Safety policy and its implementation will be reviewed annually.

Review in December 2020

Due to the pandemic resulting in school closure, the children have been engaged in more on-line learning, and communication between parents and teachers has been mainly electronic (email, google Classroom or Seesaw) or by telephone.

Rosetta has agreed the following home learning policy, which is relevant to this policy

1. All on-line communication must be as polite and respectful as face to face. The guidance in the school's Social Media Policy (available on the school website www.rosettaps.co.uk) must be followed.
2. If there is a period of school closure, both on-line and off-line learning activities will be provided. Parents may be asked to come to school to collect learning packs.
3. If the class is self-isolating, teachers will post a message each morning as to the work that should be completed that day. However, if a teacher is ill, they will not be working from home, and another teacher from the year group or key stage will set work.
4. Children are expected to engage with their learning tasks on a daily basis. Parents are asked to contact the class teacher if there are issues (perhaps health related) or difficulty accessing on-line learning. The teacher will alert the Head of Key Stage and/ or Principal if there is no engagement, and the parents will be contacted.
5. Teachers will respond to communication from parents and children during their working day. They will respond in a timely fashion, but an immediate response is not always practical.
6. Digital homeworks must be submitted, the teacher will give options if the parent has notified them that access to appropriate technology/ internet access is problematic.
7. Online learning posted on Seesaw or Google Classroom must not be shared outside of these platforms.

Follow these SMART tips when online

S

Secret - Always keep your name, address, mobile phone number and password private - it's like giving out the keys to your home!

M

Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

A

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages.

R

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

T

Tell your parent or carer if someone or something makes you feel uncomfortable or worried

Computer and iPad rules

- On the C2k network, I will only use my own login username and password.
- I will only access my own personal files. I will only access someone else's if they have given me permission.
- I will use the Internet for research and school purposes only.
- I will ask permission before entering any website, unless my teacher has already approved that site or has asked me to do independent research.
- I will immediately report any pop-up boxes which I do not understand.
- I understand that I am not allowed to enter Internet Chat Rooms or Social Networking Websites while using school computers or iPads.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I will leave all electronic devices and memory sticks at home unless instructed by my teacher.
- I will only print out documents with my teacher's permission.
- I will treat all equipment with respect and report any breakages to my teacher.
- I understand that breaking any of these rules may result in me not being allowed to use the Internet, computers or iPad.



