E-safety agreement form: parents

Recreation Road Infant School

Parent / guardian name:……………………………………………………..

Pupil name: ………………………………………………………………….

Pupil's class: …………………………………

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school.

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

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour.

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

Parent's signature:…………………………………………. **Date:**………………….

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

Recreation Road Infant School

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all adult users are aware of their responsibilities when using any form of ICT. All such users are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with *Headteacher.*

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

- ➢ I understand that it is an offence to use a school ICT system and equipment for any purpose not permitted by its owner.

- ➢ I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted 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 understand that I am responsible for all activity carried out under my username

- ➢ I will ensure that all school generated electronic communications are appropriate and compatible with my role.

- ➢ I will only use the approved, secure email system(s) for any school business

- ➢ I will ensure that all data is kept secure and is used appropriately and as authorised by the Head teacher or Governing Body. If in doubt I will seek clarification. This includes taking data off site.

- ➢ At school, I will not install any hardware or software without the permission of *Headteacher.*

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

- ➢ Images will only be taken, stored and used for purposes in line with school policy and with written consent of the parent, carer or adult subject. Images will not be distributed outside the school network/learning platform without the

consent of the subject or of the parent/carer, and the permission of the Head teacher.

➢ I understand that my permitted use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

➢ I will respect copyright and intellectual property rights.

➢ I will report any incidents of concern regarding children's safety to the Senior Designated Professional or Head teacher.

User Signature

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

Full name:…………………………………………………………….…(printed)

Job title:…………………………………………………………………….…

Signature:……………………………………………………**Date**

Recreation Road Infant School
E-Safety Policy

Writing and reviewing the E-safety policy

The E-safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- ➢ The school will identify a member of staff who has an overview of E-safety, this would usually be the Senior Designated Professional (SDP).

- ➢ Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.

- ➢ The E-safety Policy and its implementation will be reviewed annually

- ➢ The E-safety Policy was discussed by Staff in June 2012………………………..

- ➢ The E-safety Policy was discussed by the Class Councils In June 2012

- ➢ It was approved by the Governors on: ……………………………………….

Teaching and learning

Why Internet and digital communications are important

- ➢ The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- ➢ Internet use is a part of the curriculum and a necessary tool for staff and pupils.

- ➢ The school Internet access is provided by …ICT Solutions… 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.

- ➢ Pupils will be educated in the effective use of the Internet

- ➢ Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- ➢ The school will seek to ensure that the use of Internet derived materials by staff and by 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.

- ➢ Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Managing Internet Access

Information system security

- ➢ School ICT systems security will be reviewed regularly

- ➢ Virus protection will be updated regularly

- ➢ Security strategies will be discussed with the Local Authority

E-mail

- ➢ **Pupils and staff may only use approved e-mail accounts on the school system.**

- ➢ 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.

- ➢ Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.

- ➢ Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- ➢ The school will consider how e-mail from pupils to external bodies is presented and controlled.

- ➢ The forwarding of chain letters is not permitted.

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.

➢ *The Headteacher* will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing photographs, images and work

➢ Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.

➢ Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

➢ Written permission from parents or carers will be obtained before photographs or images of pupils are published

➢ Written permission from adults will be obtained before their names, photographs or images of themselves are published

➢ Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing on the school learning platform

➢ The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.

➢ Newsgroups will be blocked unless a specific use is approved.

➢ All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

➢ Pupils must not place personal photos on any social network space provided in the school learning platform without permission.

➢ Pupils, parents and staff will be advised on the safe use of social network spaces

➢ Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

➤ The school will work in partnership with Norfolk Children's Services to ensure systems to protect pupils are reviewed and improved.

➤ If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff.

➤ The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

➤ Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet **(1)**.

➤ 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.

Other devices

➤ Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. Taking photographs at any time without the subject's consent will be discouraged.

➤ The sending of abusive, offensive or inappropriate material is forbidden.

➤ Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.

➤ Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

Protecting personal data Protecting personal data

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

(1 This is under review)

Policy Decisions

Authorising Internet access

> All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.

> Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the Internet on the school site.

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 Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.
> The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and 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 referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with school child protection procedures.

> Pupils and parents will be informed of the complaints procedure.

> Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

> All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communications Policy

Introducing the E-safety policy to pupils

➢ Appropriate elements of the E-safety policy will be shared with pupils

➢ E-safety rules will be posted in all networked rooms.

➢ Pupils will be informed that network and Internet use will be monitored

➢ Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

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' and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.

➢ Parents and carers will from time to time be provided with additional information on E-safety.

Signed…………………………………………………………..Headteacher

Signed…………………………………………………………Chair of Governors

Date………………………………………….