ORCHARD LEA JUNIOR SCHOOL

E – Safety and ICT Acceptable Use Policy

This policy applies to all staff at Orchard Lea Junior School.

E – Safety and ICT Acceptable Use Policy

1. Introduction
Our E-safety and ICT Acceptable Use Policy (AUP) has been written by the ICT C0-ordinator, in the light of the Kent NGfL policy, Hampshire LA and government guidance. It will be reviewed annually.

Use of the School's ICT equipment by any members of the school community must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the School Governing Body.

The Policy will be distributed to all members of the teaching staff, any group who might use the computer suite and displayed on the website for parental viewing.

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

3. Using the Internet to Enhance Learning
The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of the students.

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use and use of online resources.

4. The need for students to learn to evaluate online content.
It is our intention to protect our pupils from inappropriate or undesirable material. The following criteria define inappropriate or undesirable materials.

- Obscene, offensive, illegal or inaccurate
- Pupils should not feel or become uncomfortable, threatened or worried by material or information on websites or from email.
- Similarly pupils must not harass, insult or attack others, violate copyright, or trespass in others' folders.

If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the school office. Internet access is via Hampshire LA's filter.

Whilst at home children may report an activity which makes them feel uncomfortable to an adult or Child Exploitation and Online Protection Centre (CEOP) or wait to inform their teacher when they return to school. They may wish to also contact the NSPCC or Childline.

The school should ensure that the use of Internet derived materials by staff and by students complies with copyright law.

5. The Management of School e-mail
Students may only use approved e-mail accounts on the school system.

Students must immediately tell a teacher if they receive offensive e-mail.

Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.

6. Management of the School Website Content
The point of contact on the website should be the school address, school e-mail and telephone number. Staff or students' home information will not be published.

Website photographs that include students will be selected carefully and will not enable individual students to be clearly identified.

Students' full names will not be used anywhere on the Website, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of students are published on the school website.

7. Management and use of online resources
Orchard Lea School recognises the importance of encouraging access to learning in the many different environments that members of the school community operate in, within school, at home or on the move.

Orchard Lea also recognises the importance of encouraging pupils to explore the issues surrounding cyber citizenship with a safe, recorded and monitored environment.

Homework
On occasions teachers may provide homework on online. Pupils who don't have internet access at home should be sensitively offered the choice of a worksheet or a pass to complete their homework using a school computer at break and lunchtime.. If a pupil has expressed a desire to use the school network then this arrangement can be assumed to be continual

Password Security
Each individual is responsible for the security and use of their username and password. You are not allowed to use the account, username or password of any other user. You must not disclose your username or password to anyone else (exception being a younger pupil with their parents). All users are responsible for all activity that occurs on their online account. If a user suspects that another has their password either because it has been stolen or given, it is the users responsibility to change their password and seek help.

8. The Management of Newsgroups and E-mail Lists

Newsgroups will not be made available to students unless an educational requirement for their use has been demonstrated.

The use of video conferencing facilities in school will be approved activities and all such use by groups of students will be monitored.

9. The Management of Chat Rooms

Students will not be allowed access to public or unregulated chat rooms.

Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.

10. Management of Emerging Internet Applications

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones will not be used without permission during lessons or formal school time, pupils may only bring in phones with written permission from parents and must leave them in the school office.

11. The Management of Internet Access

The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.

Parents will be informed that students will be provided with supervised Internet access.

Students must apply for Internet access individually by agreeing to abide by the Responsible Internet Use statement.

Parents will be asked to sign and read with their child and return a consent form.

12. The Management of Risk Assessment

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. 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. Neither the school nor Hampshire LA can accept liability for the material accessed, or any consequences of Internet access.

13. The Management of Content Filtering

The school will work in partnership with parents the, DfES and the Internet Service Provider to ensure systems to protect students are reviewed and improved.

If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the school office and Hampshire IT.

14. Informing Students about the AUP

Rules for acceptable use will be posted in all rooms where computers are used and using the interactive white boards.

Students will be informed that Internet use will be monitored.

Instruction in responsible and safe use should precede Internet access.

15. Staff Consultation

All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.

All staff including teachers, supply staff, classroom assistant, administration, caretaking staff, and Governors will be provided with the School Internet Policy, and its importance explained.

16. Maintaining the ICT System Security

The school ICT systems will be reviewed regularly with regard to security.
Virus protection will be installed and updated regularly (Agile IT)

17. The Management of Complaints Regarding the Internet

Responsibility for handling incidents will be delegated to a senior member of staff.

Any complaint about staff misuse must be referred to the headteacher.

18. Enlisting Parental Support

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

19. The Management of Community use of the Internet

 Adult users will need to sign the acceptable use policy.

Parents/carers of children under 16 years of age will generally be required to sign an acceptable use policy on behalf of the c

Orchard Lea Junior School
Responsible Internet Use

Rules for Staff

- The school computer system provides Internet access to pupils and staff. This Responsible Internet Use statement will help protect pupils, staff and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.

- School computer and Internet use must be appropriate to the pupil's education or to staff professional activity.

- Copyright and intellectual property rights must be respected.

- Users are responsible for e-mail they send and for contacts made.

- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.

- Anonymous messages and chain letters must not be sent.

- Chat rooms are allowed only through the Virtual Learning Environment (VLE).

- The school ICT systems may not be used for private purposes, unless the headteacher has given permission for that use.

- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.

- Data storage devices may be used only in accordance with the Internet Acceptable Use Policy.

- Irresponsible use may result in the loss of Internet access.

- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

- Images of children attending our school should only be used if parental agreement has been given and should never be named.

- Pupil information should only be sent to other organisations via Hants.Web.

- Teachers will inform children about safety and at all times promote the safe use of the Internet with pupils.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Orchard Lea Junior School
Responsible Internet Use

- I will ask permission before entering any Web site, unless my teacher has already approved that site.

- On a network, I will use only my own login, or class login and password, which I will keep secret.

- I will not look at or delete other people's files or download programs onto school computers.

- The messages I send will be polite and sensible; I will not post negative or personal comments about another person on the internet.

- Whilst on the computer, I will not give my home address or phone number, or arrange to meet someone and will abide by the rules learnt in school about using the internet safely.

- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher, another suitable adult or report it to CEOP if appropriate.

- I know that the school may check my computer files and may monitor the Internet sites I visit.

- I understand that if I deliberately break these rules I could be stopped from using the Internet or computers.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.6