Drayton CE VC Junior School
E-Safety Policy

AIM
To ensure that all members of the school community are appropriately protected from E-Safety related issues.

INTERNET ACCESS AND FILTERING
The school Internet access is designed expressly for pupil use and includes filtering appropriate to the needs of the curriculum. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities.
Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
The schools will endeavour to ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
The school will work with ICT Solutions to ensure that systems to protect pupils are reviewed and improved. The Headteacher will be made aware of filtering profile changes by ICT Solutions.
If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator and / or ICT Solutions. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP and ICT Solutions.

NETWORK SECURITY
The security of the school information systems will be reviewed regularly by the Computing Subject Leader, the Headteacher and the ICT Technician. Virus and Spyware protection is installed and updated regularly by the ICT Technician. Further security strategies will be discussed with ICT Solutions.
Login details must not be shared. All pupils are taught the importance of this.

EMAIL
Pupils may only use approved e-mail accounts in school, in this case the county provided Googlemail addresses. 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.
E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

WEBSITE
The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. The head teacher, Computing Subject Leader will take overall editorial responsibility and ensure that content is accurate and appropriate.
Images that include pupils will be selected carefully. Pupils' full names will not be used on the website particularly in association with photographs. Written permission from parents or carers will be obtained before images of pupils are electronically published.
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
All staff must read and sign the 'Acceptable Use Policy for Computing' and read the guidance before using any school Computing resource.

E-SAFETY COMPLAINTS

Any issues should be reported immediately to the Computing Subject Leader or the Headteacher. Any online evidence of an issue should be collected as soon as possible. Where necessary the complaints policy and disciplinary procedures will be followed. E-safety incidents outside school involving staff or pupils will be dealt with individually, depending on their impact in school.

.

USING THE INTERNET IN THE COMMUNITY

Students with outside access (e.g. on work experience) need to follow both the school's E-policy and any applicable to the placement.

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

TEACHING E-SAFETY

Instruction in responsible and safe use should precede Internet access. Pupils should be made aware of what to do should they have an e-safety concern. e-safety rules will be posted in rooms with Internet access. Users will be informed that network and Internet use will be monitored.

As part of the computing curriculum (from September 2014), every Year group will be taught e-safety skills as part of their Computing or PHSE lessons. All staff are to inform pupils of any e-safety issues that relate to an activity.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

PARENTAL SUPPORT

Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.

GUIDANCE FOR STAFF ON THE APPROPRIATE USE OF FACEBOOK AND SOCIAL NETWORKING SITES

The school strongly advises that professional and personal links with parents are kept separate but recognises that for some staff, these relationships cannot be separated. However, staff must be vigilant with what they place on Facebook, Twitter or any other public Social Networking sites.

Staff should:-

- Check security settings on Facebook
- Consider which parents you accept as friends
- Care must be taken with comments placed on Social Networking sites. They should not mention Drayton CE Junior School or any events at Drayton CE Junior that should remain confidential and/or could portray the school negatively (This includes comments on other people's postings which can be seen by a wider audience than your friends).

Our e-Safety Policy has been written by the school, building on the NCC e-Safety Policy and government guidance.