Ripple Primary School

Policy Statement for the Acceptable Use of the Internet (AUP) and security
Mission Statement

At Ripple Primary School we are proud to provide a safe, stimulating and inclusive learning environment where every member of our community is valued and respected. We listen to each other and every voice is heard.

Our broad, balanced, creative curriculum and enrichment activities provide opportunities for all to achieve and succeed.

We celebrate our achievements, differences and cultural diversity. Together we take pride in making a positive contribution to our school and the wider community.

Rationale

Acceptable Use Policy for Schools:

It is a condition of Internet access through the LA, and a condition of grant funding through the Standards Fund, that schools adopt the LA's Acceptable Use Policy. All adults and children who use the CC4 network are required to sign that they accept the Acceptable Use Policy.

Purpose

While there are dangers associated with the Internet, the Internet provides access to a vast range of information. Quoting from Stop! Think! Go? Internet Proficiency formally produced by Becta, DfES and QCA:
The Internet enables access to a vast range of cultural, scientific and intellectual material, which might otherwise not be freely or readily available. It extends the school's walls, to museums, galleries, organisations of every kind and displays them.
This Acceptable Use Policy (hereafter known as AUP) is designed to ensure that both pupils and aults use the Internet safely and responsibly as an integral part of their learning at school. The policy therefore takes into consideration the responses made by all adults connected with the school as well as government and other recognised authorities on Internet safety.

Guidelines

Parental Permission:

1. Internet Usage:
    a. No pupil should use the Internet in a Barking and Dagenham School without parental permission, and without accepting the school's rules on acceptable use that they click to accept or decline at every log on. The Internet Permission Form will form part of the home-school partnership agreement. This acknowledges that parents and carers accept some responsibility for the way in which their children use the Internet and that, in spite of all reasonable precautions and supervision, there still remains a small risk of children viewing inappropriate material
2. Photographs of Pupils:
    a. Parents received a letter and were asked to return the letter if they were against photographs being taken of their children. In other words, they were required to opt out rather than opt in to this agreement. Some parents have expressed their desire that their children not be photographed although the vast majority have not

A Filtered Internet Service:

RM provide a filtered Internet service to schools that currently filters out websites known to contain racist, offensive, pornographic, illegal or other inappropriate material. Ripple Primary School has

requested permission to manage the filtering of sites not permanently blocked by RM and that permission has been granted. It is the Network Manager's responsibility to grant or continue to deny access to certain sites using the tool from RM. Staff members wishing for access to a site that is blocked will contact the Network Manager who will review and take appropriate action on a case-by-case basis.

It is important to remember though that no filters are ever 100% effective. It is the responsibility of all teaching and non-teaching staff as well as pupils to report instances of inappropriate sites not being filtered so that they can be blocked. This information must be reported immediately to the Network manager and Head teacher.

A Common sense Approach:

- Many of the risks of using the Internet and related technologies can be minimised by taking a common sense approach by all adults involved in helping children learn:
- At home, computers should be in areas with open access, where everyone can see what is on screen
- The school has implemented the **SAFE** approach to Internet Safety
    - **Keep** personal information **SECRET**
    - **ATTACHMENTS** might contain computer viruses. **Be careful!**
    - If you **FIND** anything that upsets you always **tell an adult**
    - **EVERYONE** is invisible on the Internet! They might not be who they say they are so **check and phone**
- Posters and leaflets are in the ICT suites reinforcing the message of safety
- Take an interest in the Internet and regularly discuss what children see and use. Focus on the positive wherever possible
- Monitor on-line time and be aware of the nature of work being completed on the web
- Educate the children to use the Internet in a sensible and responsible manner
- Warning children that there are some unsuitable sites on the Internet and discussing the issues involved
- Make children clear of the consequences for misuse of the Internet and technologies present both within the school and at home

Supervision:

Within the classrooms pupils must be supervised when using a computer. Within more open areas and outside, it is accepted that children might not be supervised directly and that nearby staff will share this responsibility. This will certainly be the case with the use of laptops since they provide a wireless connectivity to the Internet and there are likely to be times when the children are not directly supervised. It is the responsibility of the teacher to make the decision as to whether the children can be trusted to use the wire connectivity safely and appropriately.

Responsibilities of Children:

The school makes use of guidelines produced by the borough for Internet use by pupils. All children must be taught about acceptable and responsible use of the Internet and should be made aware of these class rules:

1. Children can only use the Internet at school if their parents agree and in so doing must use it responsibly.
2. Children must always get permission from a member of staff before using a computer.
3. Inappropriate materials must not be sought and if any are discovered they must be reported to an adult immediately and the site will be reported to the ICT coordinator/technician for reporting to the internet filter site
4. Children must not use the Internet unsupervised and must not download programs since these could contain spyware that leads to a slowdown in processor power and can render the computer almost unusable. Spyware companies are developing more and more strategies to get children to click. Children are reminded about being SAFE but the school wishes to be more proactive in preventing the accumulation of spyware on computers. The school uses Sophos Antivirus software that contains anti-spyware. The servers are scanned automatically every night and any spyware or viruses are automatically removed.
5. It remains unlikely that there would be any particular kind of cyber bullying in Ripple Primary

school. Never the less, this could occur. All members of Ripple Primary School are responsible to show care, consideration and respect for each other at all times, whatever the circumstances. To date there has been no record of cyber bullying and it is our intention that this remains the case

Guidelines for Specific Technologies:

Chat-rooms, Discussion Groups & Instant Messaging (IM), Web 2.0 technologies:

1. Children are not allowed to enter or access the above within school. Please refer to SAFE when educating your children at home
2. Real Time Conferencing (NetMeeting):
    a. Real Time Conferencing will only take place within school under direct adult supervision during lesson time
3. Email:
    a. Children are not allowed to access their home-based email accounts within school. The School will provide children with a class email account e.g. **Y6a@ripple**.... if it is needed. Such examples would be for sending and receiving email from the children in Trewern or liaison with another school. Children will be reminded not to divulge personal information via email and will be warned that email must be used in accordance with SAFE, common-sense thinking:
    b. Email is only for sending appropriate information to the intended recipient
    c. Computer viruses are spread mostly via email so be very careful when you receive an attachment and keep your computer's antivirus software up to date (the school's machines do this automatically) We will also offer advice via the school's web site of serious virus outbreaks and a suggested plan of action
4. Web 2.0 technologies (these are collaborative technologies on the Internet. Examples of Web 2.0 technologies include blogging, podcasting and wikis.) For an explanation as to what these technologies are please see the end of this document
    a. Blogging:
        i. Children are allowed to post topics of conversation as well as reply to other children's or staff members' topics. The school's blog site is http://rippleprimaryschool.blogspot.co.uk
        ii. At all times the topics posted by the children must be checked for appropriateness by the teacher or staff member responsible. If any topic is posted that is potentially upsetting in any way then it is to be immediately deleted and any further appropriate action carried out. To date, no inappropriate topics have been posted (Feb 2012)
        iii. At all times the comments in reply to the posted topics must be checked for appropriateness by the teacher or staff member responsible. In the majority of cases it is likely that the Network Manager will authorise or deny the posting of comments, as there is an RSS feed that alerts the Network Manager to all comments made on posts. If any comment is posted that is potentially upsetting in any way then it is to be immediately deleted and any further appropriate action carried out. There have been occasions (still the vast majority of comments made are perfectly acceptable in terms of appropriateness) where it has been necessary for comments to be refused through in appropriate language. In these cases it was possible to record the IP address of the computer used to send the message. The Network Manager will monitor and record these addresses wherever it is possible to tell the address
        iv. Children may post or comment anonymously if they so wish or they may post or comment using their first name only
    b. Podcasting:
        i. Podcasting means that children's voices may ultimately be published onto the Internet. There is no way, though, to identify the child providing the following is adhered to;
        ii. Children may publish their podcast using their first name only or the class name and particular topic etc. The point being made is that children must not use their full name
5. PDAs
    a. The PDAs aren't CC4 built (they can't be) and therefore operate without any user control.

It is therefore essential that the children use the PDAs supervised, no files are downloaded without staff permission and all of the conditions associated with the acceptable use of the Internet are maintained

6. Asus minibooks
    a. Both Junior Buildings at Suffolk Rd and the Infant Building, Suffolk Road as well as Level 3 classes, Westbury each received a trolley (Minibus) with 30 Windows XP Asus minibooks. These devices are *not* CC4 built. Again, children must use the Asus minibook in strict accordance to this document: no downloading files without permission; only accessing sites that are suitable; using the software in a responsible manner
    b. The latest Asus minibooks (May 2012) that are soon to be available for use by pupils and staff at the Westbury Site *are* CC4-built making control over what can and can't be done in agreement with current practice. Cost permitting, it is the intention to make all Asus minibooks CC4-built
    c. (Update: May 2016) It is currently the intention to replace the Asus minibooks since they are no longer fit for purpose.
7. Pupils must only log on to the server or the Learning Gateway using the generic username and password that they have been given by the staff or with their own username and password. On no account must anyone try to found out passwords in order to gain access to a personal account. This is a serious breach of security and will be treated as such in the event of this ever happening. To that end, if people discover other people's passwords the Network Manager is to be informed and the password to the account must be changed

Responsibilities of Staff:

All staff must be made aware about acceptable and responsible use of the Internet and agree to adhering to this AUP.
(Update 2014) As soon as a new staff member signs on, they are presented with the AUP, which they must click to accept the agreement otherwise they are immediately logged off. Every few months the AUP reminder appears for all staff; again, they must click to accept the terms agreement otherwise they are automatically logged off. Administrators must sign the agreement every time they log on.
Whenever there is an amendment to the AUP, the AUP will appear at logon and staff must agree to the AUP otherwise they are immediately logged off.

Inappropriate Materials:

- Staff must never knowingly seek to view material over the Internet that is illegal, pornographic, sexist and racist or in any way offensive to minorities or that would be considered unsuitable within a school environment. This includes those sites that may display images and other material in poor taste, and jokes that are aimed at an adult audience. It is acceptable to use the Internet in school for social or personal activities

Photographs / videos of Children:

- Staff are required to ensure that parental permission has been granted before taking or using an image of a pupil. Electronic images of children remain school property and should be used for school purpose only. However, productions can be videoed and sold to parents as a keep-safe. Photographs and videos of children are stored on the RMStaff partition thereby preventing pupil and non-staff member access. This is also non-accessible from outside of the school

Children on School Websites:

- It is the school's duty to ensure that every child in their care is safe and, accordingly, it is important that no individual child is able to be identified or contacted by visitors to the school's website. Consequently, school websites should **not** include:
    a. Full name details or names of any child in a photograph

Individual photos of any child will be used with caution.

Chat-rooms, Discussion Groups & Instant Messaging (IM):

- Access is perfectly acceptable; in accordance with accepted practice computers must be locked (if the member of staff must leave immediately), logged off or the classroom locked thereby preventing pupil access to such sites

Email:

- The borough has recently switched to Office 365 for its email solution. Office 365 requires a strong password of at least 8 characters. All new staff joining since the introduction of Office 365 have been given a CC4 password that is the same as their Office 365 password. As with all passwords, staff are expected to ensure that it remains confidential but may be given to the Network Manager to assist in email diagnosis if so needed.

- Many staff have requested that they have access to email on their smart phones. Staff with compatible phones have been made aware of apps such as OWA for accessing email. OWA requires a password to open it.

- Staff and Governors must only use the Office 365-provided email address in all correspondence with the school and its members

E-Policy agreement:
All staff and pupils are to sign an e-Policy agreement that adheres to this AUP. This is a new expectation.

Using the CC4 Server:
In order to preserve and maintain school resources in safe and secure order, all CC4 and Learning Gateway passwords must be kept secure and remain confidential to the user and Network Manager. If there is any breach of password security the password must be changed and the Network Manager immediately informed. If staff are unsure/unaware of their password please inform the Network Manager immediately and a new password will be issued and the staff member informed of the new password. Staff are also reminded to save files into the correct drives on the CC4 server. In some cases this will be to the RMStaff network drive and at other times the RM Shared Network drive. At no time must information that is not freely acceptable to all be placed on the RM Shared Network drive (e.g. photographs of children, reports).

Downloading Files & Attachments and Virus Awareness:

- Since the school uses Sophos Antivirus that automatically updates itself to carry the latest virus detection engine, downloading files from the Internet is generally safe. However, there are risks in that some programs can slow the system down to such an extent that the computer is almost too slow to use. This is caused by the downloading of what is known as spyware. The user will not know that the program is spyware, however. It is important to recognise that spyware are not viruses but they do impact upon the computer processor and can lead to the propagation of SPAM. Therefore, staff are reminded that the installation of 3rd party software is not permitted unless agreed by the Network Manager
- Again, because of the presence of Sophos Antivirus emailing files is generally safe. However, the main means by which viruses are now spread is by email. The school has followed the LA's advice and all school computers have installed Sophos antivirus that automatically receives updates from the server
- Sophos antivirus is installed on staff home PC computers that have requested it or another suitable antivirus program has been installed. That way whenever there is a major virus outbreak the computers will already be protected with the appropriate IDE files.

Privacy on the server:

- Although staff, pupils, parents and the wider community are permitted to save personal files within their own password-protected area of the CC4 server, ultimate possession of this data lies with School and if necessary those staff members with the appropriate rights will access and if necessary delete the information.

Legal Considerations:

- Certain behaviour is clearly illegal, such as using a computer to perpetuate credit card fraud, to deliberately spread viruses, to hack or gain access into other computers without due and considered reason or to download copyrighted materials. Such issues are covered by the Computer Misuse Act 1990, the Data Protection Act 1998 and copyright legislation.

Access to the school server from outside the school

Access to the school server from outside the school is, at present, not possible. It is intended that there

will be access to the server as soon as possible. (Feb 2016)

Responsibility of Parents

Parental involvement can help reinforce the messages of Internet safety and extend the learning progress into the home. Parents must return the “Internet Permission and Photograph Consent Form” specifically identifying what their child can and can’t be involved in if they do not wish their child to participate. They must also sign and return the “e-Safety Home/School Agreement Form”.

_____

S Long March 2004 updated Sept 2004 updated Jan 2006 updated May 2008 updated Feb 2010

S Long / B Davis / C Steggle Updated Feb 2012 Updated May 2012

S Long / B Davis / C Steggle Updated April 2013 Updated October 2013

S Long / C Steggle – Updated May 2016