THAMESVIEW SCHOOL

Thong Lane, Gravesend,

Kent DA12 4LF

Acceptable Use Policy (AUP)

ACCEPTABLE USE POLICY FOR STAFF AT THAMESVIEW SCHOOL

Purpose;
The purpose of this policy is to give guidance and support to all staff members in the school who have access to the school computer system, including internet and email. Staff can use this policy to try and make work practices more effective and efficient.

Aims;
The school aims to provide staff with computer access to enable them to work in a more efficient manner, however, there needs to be a coherent set of expectations that all staff members have a clear understanding of.
Technology is an excellent tool for teaching and learning, and the benefits far out way the risks associated with internet or email use.

1. Staff Use of the School's Internet Service

This policy applies to any device used by an adult or student which is either school owned, or is their own personal device.

a) The school management wish to encourage the use of email and internet by staff in support of their work and professional development.

b) Whilst staff are encouraged to use email and the internet in support of their work all use of these facilities should be appropriate to the work, standards and ethos of the school.

c) The use of the schools internet and email systems are not provided as a 'right' to any of their users. They may be withdrawn from any user (adult or pupil) who does not conform to this Internet and Email Acceptable Use Policy

d) The school is responsible for authorising any user of its internet or email facilities, monitoring and policing their use.

e) Any member of staff who commits a serious offence in the use of the schools Internet service may be subject to the school's staff disciplinary procedures. **An example of a serious offence can be found in Appendix 1.**

f) Any user, adult or student, who breaks the law in respect of using the school's Internet service will be reported to the police.

g) Never pass on, make obvious, or leave in an insecure place, any passwords associated with using the Internet, e-mail or computer system.

h) Be aware of giving personal details, information, images or contact details of your own, or any other person, to Internet sites including weblogs, forums, social networking sites or chat rooms. At all times comply with the **Data Protection Act**.

i) If you see any unacceptable site or material as a result of an innocent Internet query, unsolicited pop-up window or in any other way, report it immediately to your line manager and e-safety co-ordinator. Action can then be taken to block the site or material.

j) Staff or approved adult school users should at all times abide by the ***copyright laws*** in respect of documents and materials downloaded from the Internet. Creative commons images and documents are available to use as they have no copy right applications. (You can search these by using http://search.creativecommons.org/)

k) Staff using a school Laptop or other device off the school site, at home or elsewhere, will still have to abide by the school Internet Acceptable Use Policy. Colleagues will be aware that the misuse of such devices for activity not agreed by the school may be breaking the law under the ***Computer Misuse Act 1990.***

l) Never upload an image to a web site without complying with the School's guidance on images loaded to the Internet.

m) Staff will at all times work to maximise the safety of students within their care in their use of the Internet

n) The school will maintain a record of all staff and students who are provided Internet access via the school's Internet service. This record will be kept up-to-date and be designed to handle common eventualities such as a member of staff leaving or a pupil's access being withdrawn etc.

o) Colleagues will be aware of the ethos, standards, equalities and ethnic mix of the school and will not access any Internet material, or work with the Internet, in any way that infringes or offends these.

p) No person should be accessing personal social network sites, e.g. facebook, Twitter etc, during normal working hours, other than for justifiable teaching purposes.

q) Staff should report all incidents of concern regarding students' online safety to the Designated Child Protection Coordinator and/or the e-Safety Coordinator as soon as possible using an appropriate communication method. Staff should report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator or the designated lead for filtering as soon as possible.

r) Staff will promote e-Safety with the pupils in their care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

2. Staff Use of the School's Email Service

Using the school's email service by staff or approved adult users.

Email Acceptable Use Statements

DO

a) Check your email regularly, at least once a day.

b) Develop an orderly filing system for Emails by setting a folder system.

c) Keep a copy of all incoming business related Emails - delete all others e.g. personal Emails, SPAM etc

d) Treat the content of any Email or an attachment that you prepare in the same way as any other paper based letter or document from a legal point of view. The Laws of the land apply equally to electronic messages and documents as they do to paper documents, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information, and wrongful discrimination. The content of the Email or an attachment must never infringe the law of the land**.** Remember it is easy for your Email to be passed on electronically to others should any recipient decide to do so.

e) Take care not to make a reply to a whole group when responding to an Email sent to a group of recipients unless absolutely necessary.

f) Keep Email messages as brief as possible. Brief messages are likely to get more attention from a recipient.

g) Make sure that the 'subject' field of any Email that you send is meaningful and representative of the message it contains. This will save user time and frustration. Be careful not to use student names as the 'subject' to protect confidentiality.

h) Make sure your email address is included on any contact information put onto paper-based letters or documents.

i) Remember that sending an email is similar to sending a letter on school letter headed paper. Do not in any way bring discredit or embarrassment to the school.

j) Any email received by a member of staff, which is regarded as illegal or offensive, should be reported to your line manager immediately. Similarly, any email received by a student, which is regarded as illegal or offensive, should be reported to the teacher immediately.

k) When sending an email about students it is good practice to put 'confidential' into the subject line, and use initials rather than full names.

l) Lock the screen by using ctrl+ alt+ del and then selecting lock screen when you leave your computer so that sensitive emails, files and data is protected.

DO NOT

a) To safeguard against computer viruses do not open external emails or an email attachment that look in any way suspicious. Report it to your school's IT co-ordinator for checking.

b) Do not make changes to someone else's Email and then pass it on without making it clear where you have made the changes. Not to do this is a form of misrepresentation

c) Do not copy images or any other material for use in your Email or an attachment that infringe the copyright law.

d) Do not, under any circumstances, give your email password to anyone else.

e) Do not print out all your email messages as a matter of course. Only print those for which it is an absolute necessity to do so.

f) Do not broadcast an email to any group of recipients unless it is absolutely necessary. It is very easy to do, but can be very annoying to recipients and wastes resources. Also, never send or forward chain email.

g) Do not open or send on any chain letter emails

h) Unless you are authorised to do so, do not send an email to any supplier that could be interpreted as creating a contract in any way. In general, do not use emails for contractual purposes. NOTE: Within the law, a user could send an email containing wording which may form a legally binding contract with a supplier.

i) Do not create email congestion by sending trivial messages or by copying emails to those who do not need to see them.

j) Do not attempt to read another person's email

k) Do not project your emails on the interactive whiteboard.

3. Mobile Phone Use by Staff;

a) Staff members are not permitted to send text messages or make phone calls during lesson time, when they are engaged in a role which is involved with students within, or as a withdrawal from, lessons.

b) Staff members are requested that if they do make a phone call outside of lesson/ working time, they do so in a manner that takes into consideration other people working around them, and is done in a private staff area.

c) Please switch off your mobile or switch to silent when left in the staffroom.

d) Do not give out your personal phone numbers to students or their parents without permission from your line manger.

4. Photographs;

a) Photographs taken of students should be taken on School digital cameras, and these pictures are only to be downloaded onto School owned hardware.

b) If a school owned camera is not available, then a mobile phone camera maybe used as long as the picture is downloaded immediately and then deleted from the phone. If you are on an authorised school trip personal cameras may be used and photos produced for use in the school.

c) Photos should only be uploaded to the website, or other internet sites with the permission of the line manager, and photos with students in should not be connected to a name in anyway, unless the site is secured by the school software security protocols.

d) CiC students should not be photographed, and staff should be aware of who has not given permission to have their photo taken.

5. Social network protocol;

a) If students or staff wish to set up any social network page that is related to Thamesview school they should gain permission to do so in the following ways;
   - Staff; Request permission from their line manager who will make a decision after consulting with the e-safety officer.
   - Students; Request permission from the staff member associated with the activity that the page will be about.

b) If these pages are then not used appropriately, requests will be made to have them removed from the site.

APPENDIX 1

What constitutes a serious offence?

These are examples of some issues which could be classed as a serious offence. These are only an indication of the kind of issues that could be classed as serious, and by no means represent the only offences which could be classed as 'serious'.

- Accessing inappropriate material on a school device (or your own device when connected to school systems).
  - Examples of inappropriate materials are pornographic/ gambling/ racist/ homophobic/ extremist.

- Continued use of social networking sites during school hours after being warned of its use.
- Sending abusive emails, or posting abusive comments on forums, or networking sites.
- Uploading inappropriate images, or having images on personal sites which might bring the school into disrepute.
- Posting inappropriate comments regarding the school or members of staff and students on social networking sites.

ACCEPTABLE USE POLICY (FOR STAFF)

This policy was agreed and adopted at a Governors' Meeting held on _____ *(date)*

Signed:_____ (Governor)

Signed:_____ (Headteacher)

The policy will be formally reviewed in _____ *(date)*