

# **e-safety policy**

## **Acceptable use - Students.**

- Involving students in formulating policy:
- The school recognises that accepted policies are much more likely to be adhered to than imposed ones.
- Fostering an open culture where accidental access is reported
- The use of surveillance technology such as Network Support Manager will inevitably uncover examples of where inappropriate sites have been visited. The school wishes to foster an open culture whereby students acknowledge and report examples of access to inappropriate sites so that they can be added to the banned list. Students reporting accidental hits will be given the benefit of the doubt for their cooperation.
- Clearly graduated sanctions - understood by all and fairly enforced
- It is central to the enforcement of this policy that the sanctions applied are understood by all students and are enforced by staff fairly ( see next section)

### **Anti Virus**

- Pupils will be encouraged to ensure that they have up to date anti-virus protection on their home PC's (ICT staff will direct them towards simple but free measures if finance is an issue)

### **E-mail**

- The Key Stage 3 Programme of Study includes instruction on the use of e-mail. The dangers of SPAM and the need to protect your identity when using e-mail. All students are provided with an e-mail account that they can access using web mail from remote PC's. This lessens the need for them to have hotmail or other unregulated accounts

### **Filtering**

- As part of their ICT entitlement all students will be made aware that their use of the internet is filtered to prevent access to known sites of inappropriate materials

### **Monitoring**

- As part of their ICT entitlement students will learn that all internet usage is monitored and that the accessing of a particular site can be tracked to a particular PC and user

### **Passwords and User Accounts**

- Pupils are given the option to change that password by accessing the option on a school PC. Students are reminded regularly that they are responsible for any activity that takes place on a machine logged in using their account. For this reason students are strongly advised **NEVER** to share their password with any other student.
- Students are also reminded that to use another persons' username and password without permission is an offence under the e-safety policy and will be punished within school.

### **Bullying / Racism**

- The school is well aware that the increase in use of mobile communication technologies has brought with it the potential for e-bullying. Where as in the past bullying usually stopped at the school or garden gate, the possession of mobile phones or e-mail accounts allows the bully the chance to intimidate even in the safety of home.

- School e-mails are monitored for abusive or threatening language although the use of text short cuts makes this a challenge. Students are encouraged to report all aspects of e-bullying to their tutor or head of year who will take the matter seriously.
- The school recognises that e-bullying does not exist exclusively between pupils and that staff are often targets of such abuse. Therefore communication between pupils and staff is only recommended through the use of school regulated e-mail accounts which are monitored, and no other method including social networking sites.
- Whether the bullying or harassment is of a racial nature or not the school will deal with the matter using its standard anti racist / anti bullying forms and procedures. The fact that ICT has been the vehicle will be a secondary issue that is tackled after the racist / bullying element has been dealt with.

## **Materials brought from home**

- The school encourages the targeted use of information technologies for coursework, homework and other teaching and learning activities. It also realises that with the development of USB technologies that there is ever more scope for sophisticated software to be introduced to the school network that might be inappropriate or might constitute a threat to the safety of the network. To this end the USB ports on curriculum PC's will be disabled in the bios or using the student accounts policies.
- Students are encouraged to see a member of the ICT staff if they require having materials placed in their user areas. This ensures that all devices are virus scanned and that only suitable files are transferred.
- Under **NO CIRCUMSTANCES** should a student be allowed to work unsupervised at a teacher's desk or Administration PC.

## **What constitutes an Offence against our E-Safety Policy?**

### **Lesser Offences ( Ones that can be dealt with by the school's internal procedures )**

- Copyright (inc plagiarism in exam work)
- Copying is the success area of ICT be it music tracks, photographs, text or other media, ICT has made mass production a reality for almost everybody. Students will be made aware that one persons copy is another person's loss.
- Copyright is a major problem in coursework. The problem however starts in the lower school (and before) when students are rewarded for handing in work which is clearly not that of a student of their age and ability. Staff need to stress from the first opportunity that sources need to be acknowledged and that straight copies or plagiarised work will not be given any credit and that the work will be set for doing again.
- Students offering copied and or plagiarised work as coursework will be seen by the exams officers and the member of SLT with line manager responsibility for that area and advised of the consequences to them of any further offences
- Downloading or storing unsuitable images
- Any image that portrays degradation, nudity, sexual activity and or violence has no place on our system. Students downloading and or storing any such image will be guilty of an offence and dealt with using the procedures outlined below,

- Storage includes students user areas or displaying materials stored on storage media of any sort ( CD, USB, Camera / phone memory cards ) or sent by e-mail attachment
- Misconduct with logins and user areas.
- The use of another person's user name or password without permission is an offence under the computer misuse act and will be dealt with using school procedures.
- Inappropriate use of own technology devices - mobile phones, digital cameras etc.
- Mobile phones may not be carried by students. Students doing so risk the confiscation of the phone until after school.
- Bullying, Harassment,
- As previously noted ICT may be used as the vehicle for bullying, harassment or Racist activities. ICT will be used wherever possible to analyse text for signs of racist abuse or bullying.

## **Consequences of minor offences**

- Intervention by class teacher-suspension of network access. First and foremost the immediate interception of wrongdoing by the classroom teacher is the most effective way of preventing any misuse of ICT. Staff, need to maintain vigilance in all lessons when students have access to ICT. Staff, have a full range of sanctions available to them up to and including short detentions during or after school - given 24hrs notice to parents if after school.
- Interview with School ICT Manager and / or Head of Year to assess severity. For persistent low level offences or an unsatisfactory response to teacher sanctions, staff are asked to refer students via standard feedback forms with a copy to the Head of year and School ICT manager. They will liaise and deal with the student depending upon other priorities for that student. In most cases a Letter to Parents / carers indicating the infringement and its severity and sanction will be a very appropriate way of following up any infringements.
- For infringements that are referred to the Senior Leadership team a period of Internal isolation or spell in learning support unit where e-safety work can take place is likely to be deemed as an appropriate sanction.
- Fixed term exclusions will be recommended to the Headteacher for persistent offences where the perpetrator shows no signs of modifying their behaviour or for offences of a particular magnitude such as attempted hacking of the school network or particularly defamatory or racist activities.
- Where a fixed term exclusion has been served the student and their parent / carer will be required to sign a declaration of proper usage before their user accounts are returned to them. Student's user accounts will be frozen until the matter is resolved and the punishment has been served.

## **Serious Offences (Ones that may require intervention from outside agencies including the police)**

**In the opinion of the school the following breaches of the acceptable use policy constitute serious offences.**

- Persistent Bullying / Harassment or Aggravated racism
- Serious breach of a persons privacy (blue jacking, hacking of restricted network drives or data systems - use of video on mobile devices to cause embarrassment or offence)

- Deliberate introduction of viruses to school
- Use of the school's ICT infrastructure for any form of gambling
- Blatant, deliberate exhibition of age restricted materials or websites.
- Use of the school's ICT infrastructure to procure illegal (or age limited) substances e.g. Alcohol, drugs, solvents etc
- Possession of illegal images

## **Consequences of serious offences**

- The discovery or reporting of a serious offence such as those described above will require immediate investigation by the School ICT Manager.
- The primary aim of this investigation will be to secure **ALL** evidence (to a standard that can be forensically checked).
- Where appropriate immediate the ICT Manager will request the involvement of school's child protection officer
- The school will also make reference to any current LA guidance on the issue.
- For cases where pornography of minors, aggravated bullying, or the use of controlled substances is indicated will require the immediate involvement of the Suffolk Police force.
- School discipline procedures will be decided **AFTER** advice or action from external bodies

## **Sources of further help / information**

- [www.becta.org.uk](http://www.becta.org.uk)
- [www.thinkyouknow.co.uk](http://www.thinkyouknow.co.uk)