E SAFETY & ACCEPTABLE ICT USE POLICY

E SAFETY AND ACCEPTABLE ICT USE POLICY

This policy aims to ensure that any communications technology is used without creating unnecessary risk to users while supporting learning.

I agree that I will:

- use personal data securely
- implement the schools E-learning and E-safety policies
- educate students in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- educate students in the recognition of bias, unreliability and validity of sources
- actively educate learners to respect copyright law
- only use approved e-mail accounts in school
- only use students images or work when approved by parents and in a way that will not enable individual students to be identified
- only give access to appropriate users when working with blogs or wikis etc...
- set strong passwords – a strong password is one which uses a combination of letters, numbers and other permitted symbols
- report unsuitable content or activities to the E-Safety Co-ordinator
- ensure that video conferencing is appropriately supervised
- pass on any examples of Internet misuse to a senior member of staff
- post any supplied E-safety guidance appropriately
- only store appropriate learning information on my laptop and make efforts to store sensitive data on the school server or private area on the Learning Platform
- ensure that my computer system is adequately protected against all manner of threats and misuse, including viruses and other malicious attacks
- Follow the code of conduct relating to the use of social networking sites (Appendix 1)
- Use the school's digital resources and systems for only professional purposes or for uses deemed 'reasonable' by the Principal and Governing Body
- Only use the approved school email, school MLE or other approved communication systems with students or parents/carers to communicate with them on appropriate school business
- Ensure that my use of private social networking sites/blogs does not conflict with my professional role

I agree that I will <u>NOT</u>:

- engage in any online activity that may compromise my professional responsibility
- invite or have students as 'friends' on any social networking medium
- give access or make reference to places of work, school, telephone numbers or addresses
- make reference to roles at work, job titles or confidential information
- subject colleagues to inappropriate or unwanted references whether in writing or via photographs
- browse, download or send material that could be considered offensive to colleagues
- use digital cameras or camera phones for taking and transferring images of students or staff without permission and will not store images at home without permission

- visit Internet sites or make, post, download, upload or pass on: material, remarks, proposals or comments that contain or relate to:
    - ❖ pornography
    - ❖ promoting discrimination of any kind
    - ❖ promoting racial or religious hatred
    - ❖ promoting illegal acts
    - ❖ breaching any Local Authority/School policies, e.g. gambling
    - ❖ anything which exposes children to danger
    - ❖ any other information which may be offensive to colleagues/students
    - ❖ chain letters
    - ❖ breaching copyright law

Care and security of ICT resources

I agree that I will

- Treat all ICT resources with due care
- Make all efforts to keep school ICT equipment secure
- Ensure all portable devices are kept locked away when left unattended during the school day and if left on the school premises overnight
- Be responsible for the insurance and replacement of portable devices in my care outside of school
- Be responsible for internet security of portable devices when used outside of school
- Ensure any data storage devices, e.g. external hard drives or pen drives and any software are virus scanned before use on the school network and laptops
- Be responsible for the content of all files and software that is personally loaded onto ICT portable devices (software and files should only be work related)
- Ensure ICT Manager has appropriate access to equipment for repair, replacement and/or maintenance as and when required
- Ensure data for which I am responsible is backed up securely either on the Network or via alternative suitable media
- Ensure that any Anti virus Software is working and up to date and to report to ICT Manager immediately if it is suspected not to be so, for remedial action.
- Ensure that equipment used during lessons is checked and returned in good order
- Report any faults or damage to the ICT Manager
- Ensure portable ICT devices are connected to power and data supplies for overnight charging and installation updates
- Ensure that equipment is loaded and unloaded correctly to prevent damage, particularly when removing laptops/netbooks from lapsafe trolleys

DECLARATION

I agree and accept that any portable ICT device loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any ‘significant personal use’ as defined by HM Revenue & Customs.

I agree to adhere to the policy requirements, understanding that failure to do so may lead to disciplinary action and accept that my use of the school and LA ICT facilities may be monitored.

Name ……..Date ……

Please sign and return to Nick Walton, Network Manager

Appendix 1

Code of conduct for staff concerning the use of Facebook and all other social networking sites

We recognise many staff use Facebook and other social networking sites and that for some staff, these sites are an integral part of their life outside work. For those of us working with young people there are some inherent dangers in using these sites which we, as part of our safeguarding practices, need to be aware of.

This guidance is intended to help staff to become aware of best practice when using social web sites and is designed to ensure staff understand that neither the school nor workplace colleagues should be compromised by inappropriate comments or images.

The Local Authority guidance explains that staff who use Facebook or other social networks on a regular basis can unwittingly place themselves in vulnerable situations to personal and professional allegations, which in some cases may lead to a disciplinary investigation involving local authority safeguarding official and the police.

The advice to all staff is that you should refrain from putting any photographs of yourself on your home page and make sure that your security settings onto your accounts are set to maximum privacy.

It will be deemed a potential disciplinary offence should these guidelines not be adhered to.

Should any member of staff be unsure of how to interpret the E Safety and Acceptable ICT Use Policy, advice should be sought from the Principal.