COWLEY INTERNATIONAL COLLEGE

E:SAFETY POLICY

Updated March 2015

Contents

Introduction

Information and Communication Technology (ICT) is seen as an essential tool to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. At Cowley International College we have built in these technologies in order to arm our students with the skills they will need for life-long learning and employment.

The world of ICT is a fast moving environment and covers a wide range of resources including; mobile learning, web-based learning and Virtual Learning Environments (VLE) to name a few. Some of the technologies available to young people in/outside of school are:

- Mobile / Smartphone's features include; video, pictures, texts and web access
- Blogs & Wikis based on Web 2.0 technologies
- Online Forums
- Chat Rooms and Social Networking, e.g. Facebook, Ichat and Twitter
- Music and Video Broadcasting
- Laptops
- Websites e.g. YouTube
- Podcasting
- Email & BBM
- Virtual Learning Platform – Dashboard

While all these technologies are exciting and beneficial to the learner some of the web-based resources are hard to monitor and are not consistently policed. All users including adults need to be aware of the risks associated with the use of internet technologies.

At Cowley International College we take the matter of e-safety very seriously and we teach all our stakeholders to use web-based technologies safely and legally. We teach our students the appropriate behaviours and thinking skills required for safe internet use that will keep them safe in and beyond the classroom.

This Policy and associated Acceptable Use Policies (AUP) cover both fixed and mobile technologies within school (such as PC's, Laptops, PDA's, Tablets, Webcams, Smartphones, Voting Systems etc).

Roles and Responsibilities

E-safety is a very important aspect of strategic leadership in school and it is the responsibility of the Principal and Governors to ensure that the policy and practice of e-safety is embedded and monitored in our school. The named e-safety co-ordinator at Cowley International College is **Mr P A Livesey** who is a member of the Senior Leadership Team (SLT). It is the e-safety co-ordinator's duty to make sure that current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection), Local Safeguarding Children's Board and Childnet are made known to others in school.

The school’s e-safety policy will be made available by the e-safety co-ordinator to all stakeholders via the website. The e-safety co-ordinator will advise Governors and SLT of any local or national changes to guidelines.

This policy, supported by the school’s AUP for staff, visitors, governors and students, is to protect the interests of the whole school community.

Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations and must take care always to maintain a professional relationship.

E-Safety Development for Staff

- New staff receive information on arrival of all the school’s acceptable use policies and must sign and complete the relevant form before access is granted.
- All staff are made aware of the procedures that they must adhere to in the safeguarding of children within the context of e-safety and how to deal with any e-safety or misuse of ICT related technologies incident.
- All staff are fully encouraged to embed e-safety activities within their curriculum area.
- Our staff receive regular information and training on e-safety issues via training sessions.
- Staff, on leaving the school will have access to their accounts removed.

Our E-Safety Message

- The school uses ABTutor (Classroom Monitoring) Websense and SecurUs (Abuse Montoring) to monitor and enforce a strict e-safety environment for everyone who accesses a school computer, laptop, offline laptop or mobile device.

E-Safety in the Curriculum

- The school has a framework for teaching internet skills in ICT and as a discrete subject in other areas.
- Pupils are taught how to spot the signs of ‘grooming’ and the potential dangers of responding to ‘requests’.
- Educating pupils on the dangers of technologies that maybe encountered outside school is taught as part of the e-safety curriculum and undertaken informally when opportunities arise across the curriculum.
- Pupils are taught through discussion, modelling and activities of the relevant legislation when using the internet, such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are made aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also made aware of where to seek advice and help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline/CEOP report abuse button SHARP system.

- Pupils are taught to critically evaluate materials and learn effective searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- All system users are informed that network and internet use will be monitored.

Password Security

- Before accessing any computer, internet or email system, students and staff must accept and adhere to the AUP.
- Students are provided with an individual network and virtual learning platform username and password. They are expected to change the default password to an individual password of their choice and keep it confidential.
- Staff users are provided with a network, virtual learning platform and a MIS account which must meet the Council's password policy.
- If you think your password has been compromised, it is your sole responsibility to contact ICT Support (ext. 132) to get it reset. Any computer misuse by others on your account will be logged as you and appropriate action taken, which could involve disciplinary action or involved law enforcement agencies.
- Members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school's networks, MIS systems and Virtual Learning Platforms, including ensuring that passwords are kept safe, not shared and changed periodically. Staff should also make sure that **NO** machines are left unattended while they are logged on.
- When logging on or during registration, staff are aware that they should not have the screen projected for all to see; this can lead to passwords being compromised as well as data protection issues.

Data Security

Accessing school data is something that the school takes very seriously. All important data is backed up on a daily basis, but if any files are accidentally deleted then you must notify ICT support as soon as possible. Staff are made aware of their responsibilities when accessing school data and must adhere to the school's Data Protection Policy.

Managing Internet Access

At Cowley International College we understand that the internet is a great resource for teaching and learning. Anyone can view information, send messages, discuss ideas and publish material, which is an invaluable resource to education, but we must identify the risks to young and vulnerable people. All school's internet activity is regularly monitored by both the school and the Local Authority and any inappropriate use will be dealt with.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor St Helens Council can accept liability for any material accessed, or any consequences of internet access.

- The school maintains students will have supervised internet access to planned teaching material/resources via the school's fixed and mobile technologies.
- Staff will plan and preview any websites before use.
- All users must observe copyright at all times and not distribute any school software or data and must not actively download material or software from the internet.
- Any homework set that requires the students to access the internet for research should be checked and monitored by the parent.

School Infrastructure

- The school's Internet/Email access is controlled using a filtering service.
- The school also controls monitors internet access via Websense which is monitored by the Principal. As a result, staff are informed that network and internet traffic is monitored and can be traced to the individual user.
- The school does not allow staff and pupils to access internet logs for the safety of all.
- Class control systems are in place, which allows staff to control access to applications and the internet.
- If staff or students discover any inappropriate content they are advised to contact the e-safety co-ordinator for further action.
- Agilisys has responsibility to make sure that all machines in school have up-to-date Anti-Virus software.

Social Media Safeguards

Facebook safeguards:

- Access to Facebook is limited to nominated persons only. It is not available generally.

Twitter safeguards:

- Twitter is slightly more open than Facebook, allowing people to follow our brand which simply means they follow our news. People can mention Cowley in a post which they would see and we would see. This would not be shown publicly to every follower.
- Conversations are not held on Twitter and pupils are not followed back.
- If abusive/threatening messages are sent the person can be blocked from both twitter and Facebook.
- Twitter messages are filtered by D Ratcliffe, Website, Publications and Marketing Manager before posting.

All staff must adhere to the school's Social Media and Mobile Communications Policy and the Council's Social Media Policy.

Managing Emerging Technologies (Web 2.0)

Web 2.0/Social networking sites offer users a great easy to use, creative and mostly free platform to interact with others or the application. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact and culture. We encourage our pupils to think carefully both in and out of school about the way that information can be added and removed by all users, including themselves.

- We currently block by default these sites using the latest Web Filtering software and we monitor all internet and email access using Symantec Email Security.
- All pupils and staff are advised to be cautious about information they upload and information given by others. Information given by others may be misleading and not from whom they say they are.
- Pupils are taught not to display images of themselves or others from school and should not display any content that some other individual could use i.e. full name, address, mobile phone number etc. Once an image is placed online it is very difficult to be removed.
- We tell pupils only to use profiles that are private to them and to deny access to unknown individuals.
- Any incidents of bullying must be reported to the school. We keep all identity and information given confidential.
- Staff may only create blogs, wikis or other Web 2.0 spaces in order to communicate with pupils using the schools Virtual Learning Platform or other systems approved by the Principal or Governors.
- Pupils should report any online abuse through the appropriate channels which they have been made aware of, e.g. Sharp system.

Managing Email Communications

The use of email above any other method of communication is such an advantage in this hi-tech modern world, and there's no doubt that staff and pupils will have to use it at some point in their lives. Within school, email should not be considered private as all email communications to and from school are monitored for various violation of school policy.

Email without doubt offers significant benefits to staff and pupils especially when working on school based projects. In order to meet ICT levels in school, pupils must have experienced sending and receiving emails.

- All staff and pupils in school are given their own unique email address for school business only, this gives us the ability to audit emails in a secure manner.
- It is the responsibility of each email account holder to keep their password secure. For the safety of all users email communications are filtered by Sophos Pure Message and logged and reports are completed on a regular basis.
- Staff should not contact pupils or parents or conduct any school business using a personal email address.
- Pupils should only use their school email for educational purposes under supervision from a teacher.
- Any abuse of the email system/policy witnessed by staff or pupils should be reported to the e-safety co-ordinator.
- All email users must adhere to the school's e-safety policy and are reminded that they have accepted and signed an AUP. The use of explicit language and content is strictly prohibited and any violations of this rule will be severely dealt with.
- Pupils are introduced to email as part of their ICT scheme of work.
- Pupils must not reveal their personal details or those of others or arrange to meet anyone without prior permission from their parents.

- To access the school’s email system go to: cowley@sthelens.org.uk

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Existing mobile technologies such as gaming devices, mobile and smart phones are very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus can open up risk and misuse associated with communication and internet use. All emerging technologies that the school intends to use will be thoroughly examined and tested before implementation in the classroom. We choose to manage the use of the devices in the following ways so that users exploit them appropriately.

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device. Staff must following the Social Media and Mobile Communication Policy.
- Pupils are allowed to bring in mobile phones. However, the school operates a ‘not seen or heard’ policy within the school buildings.
- The sending of inappropriate text, image and video messages between any members of the school community is not allowed.

Safe Use of Images

Please see school policy on the use of images and video which is available on the college website under ‘Policies’ section.

Storage of Images

- Images of children and staff are stored securely on the school’s network.
- Pupils and staff are not permitted to use personal portable media for storage of images without express permission from the Principal.
- Access to these images are for staff or school purposes only and use on the school’s website and VLN.
- Agilisys is responsible for the deletion of images no longer in use by the school or if the member of staff or pupil has left the school.

CCTV/Webcams

- The school has a large CCTV infrastructure for the safety and security of all persons on the site. A separate CCTV policy is in use.
- Webcams are only used in school as a learning resource within ICT lessons.

Misuse and Infringements

Complaints relating to e-safety should be made to the e-safety co-ordinator or Principal.

Handling E-Safety Complaints

- All users are made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be reported immediately to the e-safety co-ordinator and action in line with the St Helens Safeguarding Children's Board e-Safety policy will be taken.
- Deliberate access to inappropriate material by any user will lead to the incident being logged by the e-Safety co-ordinator and appropriate action being taken.
- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children will be reported to the LADO (Local Authority Designated Officer) within one working day in accordance with the St Helens Safeguarding Children's Board Policy.
- Any complainant about staff misuse must be referred to the Principal and if the misuse is by the Principal it must be referred to the Chair of Governors in line with the St Helens Safeguarding Children's Board Child Protection procedures.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-Safety rules.
However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety.

Parental Involvement

Parental involvement is always welcomed at Cowley International College and we consider ourselves to have a good working and professional relationship with the parents of our pupils. We always try to encourage parents to have their say on any matter related to the school.

- Parents/Carers and pupils are actively encouraged to comment and contribute to adjustments or reviews of the school's e-Safety policy by emailing cowley@sthelens.org.uk
- Parents/Carers are asked to read through and sign an AUP on behalf of their child on admission to school.
- Parents/Carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain i.e. school website.
- The school disseminates information to parents relating to E-Safety where appropriate in the form of:
    - Information and celebration evenings
    - Posters
    - Website / Learning Platform postings
    - Newsletter items
    - Learning Platform training

Writing and Reviewing this Policy

This policy will be reviewed every three years or sooner if the school sees fit to add a change for security/safety reasons.

Review Procedure

There will be an on-going opportunity for staff to discuss with the e-Safety co-ordinator any issue regarding e-Safety that concerns them.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Related publications / information

- Internet and Email Policy including Acceptable Use Policy
- Data Protection Policy
- Safeguarding Policy (including Child Protection)
- Social Media and Mobile Communication Policy
- CCTV Policy
- www.getsafeonline.org
- www.ceop.police.uk