COWLEY INTERNATIONAL COLLEGE

E-SAFETY POLICY

Autumn Term 2019

Contents

1. Introduction

Information and Communication Technology (ICT) is seen as an essential tool to support teaching and learning in every aspect of the curriculum, 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 college are: Mobile / Smartphone's, Blogs & Wikis based on Web 2.0 technologies, Online Forums, Chat Rooms and Social Networking, e.g. Facebook, Instagram and Twitter, Music and Video Broadcasting, Websites e.g. YouTube, Podcasting, Email & BBM, Virtual Learning Platforms.

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 college (such as PC's, Laptops, PDA's, Tablets, Webcams, Smartphones, Voting Systems etc).

2. Aims

Our college aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole college community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

3. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for college's on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

4. Roles and responsibilities

4.1 Principal & Governors

E-safety is a very important aspect of strategic leadership and it is the responsibility of the Principal and Governors to ensure that the policy and practice of esafety is embedded and monitored in our college.

4.2 The designated safeguarding lead (DSL)

Mr P A Livesey is the named e-safety co-ordinator and the designated safeguarding lead for the college. The DSL takes lead responsibility for online safety in college, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the college
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the college behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in college to the Principal and/or governing board

4.3 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at college, including terrorist and extremist material
- Ensuring that the college's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the college's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

4.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the college's ICT systems and the internet. Ensuring that pupils follow the college's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the college behaviour policy

4.5 Parents

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.

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy by emailing cowley@stehelens.org.uk
- Ensure their child has read, understood and agreed to the terms on acceptable use of the college's ICT systems and internet
- Read through and sign an AUP on behalf of their child on admission to college.
- Make a decision as to whether they consent to images of their child being taken/used in the public domain i.e. college website.
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

4.6 Visitors and members of the community

Visitors and members of the community who use the college's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Educating pupils about online safety

The college has a framework for teaching internet skills in ICT. The safe use of social media and the internet will also be covered in a range of subjects where relevant.

- 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 college is taught as part of the e-safety curriculum and undertaken informally when opportunities arise across the curriculum. The college will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.
- 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.

6. E-Safety Development for Staff

- New staff receive information on arrival of all the college'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 college will have access to their accounts removed.

7. Educating parents about online safety

The college will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety may also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

8. Cyber-bullying

8.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

8.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The college will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Both ICT and TeamTeachers will discuss cyber-bullying with their groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

The college sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the college will follow the processes set out in the college behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the college will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

8.3 Examining electronic devices

College staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on

pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the college rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material
- Retain it as evidence (of a criminal offence or a breach of college discipline)
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the college complaints procedure.

9. Acceptable use of the internet in college

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the college's ICT systems and the internet. Visitors will be expected to read and agree to the college's terms on acceptable use if relevant.

Use of the college's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

10. Pupils using mobile devices in college

Pupils may bring mobile devices into college, but are not permitted to use them during:

- Lessons
- Team Tutor time
- Clubs before or after college, or any other activities organised by the college
- Must not be used on the corridors

Mobile phones should not be seen or heard in the building. If seen they will be confiscated and locked in Student Services. Mobile phones can be collected from Student Services at the end of the college day. Please be aware parents/carers maybe contacted to come into college to collect the device.

Any use of mobile devices in college by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the college behaviour policy, which may result in the confiscation of their device.

11. 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 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 college'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.

12. Data Security

Accessing college data is something that the college 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 college data and must adhere to the college's Data Protection Policy.

13. Internet Access

13.1 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 college's internet activity is regularly monitored by both the college and the Local Authority and any inappropriate use will be dealt with. The college 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 college network. Neither the college or St Helens Council can accept liability for any material accessed, or any consequences of internet access.

- The college maintains students will have supervised internet access to planned teaching material/resources via the college'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 college 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.

13.2 Equal Opportunities Pupils with additional needs

The college endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the college'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.

13.3 College Infrastructure

- The college's Internet/Email access is controlled using a filtering service.
- The college 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 college 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.
- St Helens Council provide our ICT support and have responsibility to make sure that all machines in college have up-to-date Anti-Virus software.

13.4 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 Weldon, Website, Publications and Marketing Manager before posting. All staff must adhere to the college's Social Media and Mobile Communications Policy and the Council's Social Media Policy.

13.5 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 college 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 college 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 college. 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 college 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.

13.6 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 college, email should not be considered private as all email communications to and from college are monitored for various violation of college policy. Email without doubt offers significant benefits to staff and pupils especially when working on college based projects. In order to meet ICT levels in college, pupils must have experienced sending and receiving emails.

- All staff and pupils in college are given their own unique email address for college 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 college business using a personal email address.
- Pupils should only use their college 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 college'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 college email system go to: cowley@sthelens.org.uk

14. 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 college. 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 college 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 college allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the college 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 college operates a 'not seen or heard' policy within the college buildings.
- The sending of inappropriate text, image and video messages between any members of the college community is not allowed.

15. Staff using work devices outside college

Staff members using a work device outside college must not install any unauthorised software on the device and must not use the device in any way which would violate the college terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside college. Any USB devices containing data relating to the college must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

16. Safe Use of Images

Please see college 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 college'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 college purposes only and use on the college's website and VLN.
- St Helens Council ICT support are responsible for the deletion of images no longer in use by the college or if the member of staff or pupil has left the college.

17. CCTV/Webcams

- The college 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 college as a learning resource within ICT lessons

18. How the college will respond to issues of misuse

Where a pupil misuses the college's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the college's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The college will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

19. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

20. Writing and reviewing this Policy

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

21. 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.

22. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure