2

**Fortiter et**

**Humaniter**

**PORTADOWN COLLEGE - E Safety Policy 2014**

What is E-safety?

E-Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate all members of the College community about the benefits, risks and responsibilities of using information technology.

E-Safety:

* Concerns safeguarding students and staff in the digital world.
* Emphasises learning to understand and use new technologies in a positive way.
* Is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
* Is concerned with supporting students and staff to develop safer online behaviours both in and out of school.

E-Safety can be categorised into 3 areas of risk:

* Content – being exposed to illegal, inappropriate or harmful material.
* Contact – being subjected to harmful online interaction with other users.
* Conduct – personal online behaviour that increases the likelihood of harm.

The purpose of policy is to:

* Protect and educate students and staff in their use of technology.
* Have appropriate mechanisms to intervene and support any incident where appropriate.

Thereby minimising potential exposure to the risks outlined above for all members of our College community

This policy applies to all members of the Collegecommunity (including staff, students, volunteers, parents / carers and visitors) who have access to and are users of College ICT systems, both in and out of the College.

6

This policy should be applied in the context of the other relevant College Policies and agreements:

* Child Protection Policy
* Child Protection Code of Conduct for Staff
* Pastoral Care Policy
* Anti-bullying Policy
* Acceptable Use of ICT: Student Policy Agreement
* Acceptable Use of ICT: Staff and Volunteer Policy Agreement

Roles and Responsibilities

7

|  |  |
| --- | --- |
| Governors | Responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. |
| Principal/Senior leadership Team | The Principal has a duty of care for ensuring the safety (including e-safety) of members of the College communityThe Principal and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents) |
| Pastoral Vice Principal(designated Teacher for Child Protection) | leads the E-Safety committeetakes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the College e-safety policies / documentsensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.provides training and advice for staffreceives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments |
| C2k/CapitaC2k Manager | Are responsible for ensuring that the College’stechnical infrastructure is secure and is not open to misuse or malicious attack• that the Collegemeets required E-safety requirements and any SELB, C2k or other relevant body E-Safety Policy / Guidance that may apply. • that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. |
| Teaching and Support Staff | Are responsible for ensuring that:**•** they have an up to date awareness of e-safety matters by attending relevant training and of the current CollegeE-Safety Policy and practices• they have read, understood and signed the Staff Acceptable Use Policy (AUP)• they report any suspected misuse or problem to the Pastoral Vice Principalfor investigation / action / sanction• all digital communications with students / parents / carers should be on a professional level and only carried out using official College or approved systems • students understand and follow the e-safety and acceptable use policies (AUP)• students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations• they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other College activities (where allowed) and implement current policies with regard to these devices |
| Students | * Are responsible for using the Collegedigital technology systems and their own personal devices in accordance with the Student Acceptable Use Policy (AUP)
* Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
* Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the College’sE-Safety Policy covers their actions out of school, if related to their membership of the school.
* Must never interfere with ICT equipment which is being used by members of staff.
 |
| Parents/Guardians | The College will take every opportunity to help parents understand these issues through parents’ evenings, letters, website and information about national / local e-safety campaigns. Parents and carers will be encouraged to support the College in promoting good e-safety practice and to follow guidelines on the appropriate use of:**•** digital and video images taken at College events• their children’s personal devices in the College |

Education – students

The education of studentsin e-safety is an essential part of the College’s e-safety provision. Young people need the help and support of the College to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

* A planned e-safety curriculum is provided as part of PD lessons and is regularly revisited
* Guidance will be provided within the PD programme on how to respond to cyberbullying (the use of digital technologies with an intent to offend, humiliate, threaten, harass or abuse somebody).
* Key e-safety messages are reinforced through assemblies and special events eg Internet Safety Day
* Students should be taught in all subjects to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
* Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* The **CEOP** (Child Exploitation and On Line Protection agency) reporting button is installed within the ‘My School’ VLE home page and on the College website

Bring Your Own Device

The College recognizes that on occasions, students may wish to bring their own device to carry out some of their school work. The College will allow such use with the following conditions:

* The College cannot be held responsible for the loss of or damage to any equipment which is brought into the College.
* All use of personal devices is governed by the Student Acceptable Use Policy (AUP)

Wi-Fi

Students and staff can gain access to the internet through the MERU routers locating around the College. Please note that all internet access via the C2k wireless network is monitored and filtered by C2k and acceptable use is covered by the student AUP.

As outlined in the Code of Conduct, use of personal devices including mobile phones is only permitted at break and lunch times during the school day. The only exception to this rule is when a teacher has given permission for use to enable a student to complete an activity with a clear educational goal.

Use of digital and video images

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

**•** Through the e-safety education programme, students should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at College events for their own personal use (as such use in not covered by the Data Protection Act).

• Staff and volunteers are allowed to take digital / video images to support educational aims, but the following steps should be taken:

(i) Images should only be taken on College equipment, the personal equipment of staff should not be used for such purposes. If a personal device is used, images should be transferred to the C2k network and images deleted from the personal device

(ii) Staff must take care when taking digital images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.

• Students must not take, use, share, publish or distribute images of others without their permission

• Photographs published on the College website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

• Students’ full names will not be used anywhere on a website or blog, particularly in association with photographs.

* The data capture form completed by the parents/guardians of students enrolling in Portadown College requires parents/guardians to state whether or not they grant permission for photographs of their child to be published on the College website or other on line media used by the College.

Storage of Data

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• Use student specific data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

• Transfer data using encryption (encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people) and secure password protected devices.

When student specific data (i.e. IEPs, reports) is stored on any portable computer system, memory stick or any other removable media:

**•** the data must be encrypted and/or password protected

**•** the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)

**•** the device must offer approved virus and malware checking software

16

**•** the data must be securely deleted from the device, in line with College policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the College considers the following as good practice:

* The official *C2k* email service may be regarded as safe and secure. Users should be aware that email communications are monitored.
* Users must immediately report, to the Pastoral Vice Principal – in accordance with the College policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
* Any digital communication between staff and students or parents/guardians (email, chat, VLE etc) must be professional in tone and content. Please see Netiquette guide (**Appendix 1**)
* Student names should never be inserted in the Contents line of any e-mail communication to ensure confidentiality where e-mail may pop up on whiteboard screens being used in classrooms.

If using methods outside the official C2k channels (e.g. OWA E-mail and Fronter Discussion Forums) to communicate with students; staff must follow the guidance provided below:

* The Head of Department should make an agreement with staff as to the purpose of using social media and when staff should be available to communicate with students. In doing so, the rights of staff to make a clear distinction between their work and personal life must be respected and facilitated.
* On line accounts e.g. Twitter should be established by a subject department rather than an individual member of staff. Passwords and usernames should be shared with all relevant staff.
* In promoting safe and responsible use of digital technologies staff should avoid using department social networking sites outside working hours.
* The use of social media should always be viewed as a means of complementing the teacher-student interaction within the traditional classroom setting rather than replacing it.
* All posts should be professional in both content and tone as stipulated in this policy and the staff AUP.
* Staff should not follow/befriend students in any social networking site.
* The Head of Department should deliver or arrange appropriate training to ensure all staff are confident in engaging with students on line.

Social Media - Protecting Professional Identity

The College has a duty of care to provide a safe learning environment for students and staff.

The College provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the College through limiting access to personal information:

* Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
* Clear reporting guidance, including responsibilities, procedures and sanctions

College staff should ensure that:

* They do not engage in online discussion on personal matters relating to members of the College community
* Personal opinions should not be attributed to the College or local authority
* Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The College’suse of social media for professional purposes will be checked by the SLT to ensure compliance with the E-Safety Policy.

Responding to incidents of misuse or illegal incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



LSCB: Local Safeguarding Children Board/Child Protection Support Service for Schools (CPSSS)

– 028 38341975

CEOP: Child Exploitation and On line Protection - CEOP works with child protection partners across the UK and overseas to identify the main threats to children and coordinates activity against these threats to bring offenders to account.

Other Incidents

It is hoped that all members of the College community will be responsible users of digital technologies, who understand and follow the College policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

* Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
* Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
* It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
* Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
* Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

• Internal response or discipline procedures

• Involvement by Local Authority or national / local organisation (as relevant).

• Police involvement and/or action

* If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
* incidents of ‘grooming’ behaviour
* the sending of obscene materials to a child
* adult material which potentially breaches the Obscene Publications Act
* criminally racist material
* other criminal conduct, activity or materials
* Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the Collegeand possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

College Actions & Sanctions

The College will deal with incidents that involve inappropriate rather than illegal misuse. Such incidents will indicate that the AUP has not been complied with and sanctions will be imposed. These may include loss of access to the College network/internet, detentions, suspensions, contact with parents/guardians and, in the event of illegal activities, involvement of the PSNI.

Development and Review of this Policy

4

This E-safety policy has been developed by the E-Safety working group made up of staff from a range of subject areas including ICT.The group followed guidance provided in DE Circular 2013/25 when creating this policy.

|  |
| --- |
|   |

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be in **June 2015**.

22

Further Information

Information guides on a range of social media sites and safe use of the Internet can be found on the College website: [www.portadowncollege.com](http://www.portadowncollege.com) (Info for Parents – Documents about PC)

Appendix 1

# Netiquette: a handy guide for teachers and students when learning on line

The word netiquette is a combination of ’net’ (from internet) and ’etiquette’. It means respecting other users’ views and displaying common courtesy when posting your views to online discussion groups. Please familiarize yourself with the following points:

**Behind Every Name There is a Person:**

* Respect the views of class members and what they share in class.
* Ask for clarification if you find a discussion posting difficult to understand. If you come across a posting you regard as offensive, report this to your teacher.
* Avoid sweeping generalizations. Back up your stated opinions with facts and reliable sources.
* Understand that we may disagree and that exposure to other people’s opinions is part of the learning experience.
* Be respectful of each other. Before posting a comment, ask whether you would be willing to make the same comment to a person’s face.
* Keep in mind that everything you write, indeed every click of your mouse is recorded on the network server. On the Internet there are no take backs.
* Keep in mind that you are participating in a class. Something that would be inappropriate in a traditional classroom is also inappropriate in an online classroom.

**Online Communication:**

* Be careful with humour and sarcasm. Both can easily be misunderstood!
* Review all discussion postings before posting your own to prevent repetition.
* Stay on the topic which has been identified in the initial post or heading.
* Check your writing for errors by reviewing what you’ve written before submitting it.
* Do not use abbreviations or acronyms eg BBL (Be Back Later) as many users may not know what you mean or misinterpret your comment.
* No matter what forum, writing in all capital letters is considered SHOUTING and is considered very rude. A word or two in caps is fine, but shouting is not recommended.
* Obey copyright laws. Don’t post material in a workspace or as an attachment in a discussion forum without acknowledging the source e.g. This picture was downloaded from [www.thinkuknow.com](http://www.thinkuknow.com)

Appendix 2 – Reporting Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reporting LogGroup .............................................................. | Signature |  |  |  |
| Action taken | By whom? |  |  |  |
| What? |  |  |  |
| Incident Reported by |  |  |  |
| Incident |  |  |  |
| Time |  |  |  |
| Date |  |  |  |

Appendix 3 – Record of reviewing devices/internet sites (reporting to incidents of misuse)

**Record of reviewing devices / internet sites (responding to incidents of misuse)**

|  |  |
| --- | --- |
| Group |  |
| Date |  |
| Reason for investigation |  |

**Details of first reviewing person**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

**Details of second reviewing person**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

Name and location of computer used for review (for web sites)

|  |
| --- |
|  |

**Web site(s) address / device Reason for concern**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Conclusion and Action proposed or taken**

|  |  |
| --- | --- |
| **Conclusion** | **Action** |
|  |  |

Appendix 4 – Resources

Further information on e safety issues can be obtained from the following websites:

* [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk/)

An education initiative by the Child Exploitation and Online Protection (CEOP) Centre

* [www.ceop.gov.uk](http://www.ceop.gov.uk)

The website of the Child Exploitation and Online Protection (CEOP) Centre

* <http://www.bbc.co.uk/webwise/0/>

BBC website containing a range of resources covering e-safety and how to make effective use of web resources

* <http://www.internetmatters.org/homepage.html>

This site contains some useful resources to help parents make informed choices about their children’s online safety.

* [www.getnetwise.org](http://www.getnetwise.org/)

Information about filtering programs for home use.

* <http://www.swgfl.org.uk/products-services/Online-Safety-Services>

The South West Grid for Learning is the UK’s leading organisation that supports schools and other organisations in safeguarding children online.

This Policy was approved by the Board of Governors on 14 October 2014.