Fortiter et
Humaniter

PORTADOWN COLLEGE – Online Safety Policy 2018

What is Online safety?

Online 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.

Online 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.

Online Safety can be categorised into 4 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.
- Commercial risks – being exposed to inappropriate commercial advertising, marketing schemes or hidden costs/frauds.

The purpose of this 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 College community (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. The roles and responsibilities of students, parents/carers and staff in regard to online safety are listed in Appendix 1.

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

Scope of the policy

In relation to online safety incidents that occur outside of College hours, the College will work with students and parents/carers to keep all students safe and offer educative support where appropriate.

Online safety outside College hours is primarily the responsibility of the parents/carers. The College has no responsibility and will not investigate incidents occurring outside of College hours*. However, if inappropriate activity is brought to our attention, which occurs outside of these times and has an impact on any member of the College community we will liaise with parents/carers to provide relevant support.

Any issues that arise inside College, as a result of online safety incidents outside of the College, will be dealt with in accordance with College Policies.

[*College hours include those times when students are participating in supervised official school events outside of normal school hours (9:00am – 3:35pm) e.g. sporting fixtures or school trips].

Education

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

Online 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 online 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 online 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 online 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 Online Protection agency) reporting button is installed within the 'My School' VLE home page and on the College website

Cyber bullying

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.

- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Students receive guidance within the PD curriculum on the importance of using all forms of on line communication responsibly and how to respond if they believe they have been the target of cyberbullying. Incidents of cyber bullying will be dealt with in accordance with the College Anti-Bullying Policy.

Sexting

Sexting is the sending or posting of sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the Internet. There are two aspects to Sexting:

- Sexting between individuals in a relationship
- Sharing an inappropriate image with an intent to cause distress

The UK Council for Child Internet Safety (Source: Sexting in Schools and Colleges: Responding to incidents and safeguarding Young People – UKCCIS, September 2016) refers to sexting among young people as ***'youth produced sexual imagery'*** to ensure there is clarity in dealing with this issue.

'Youth produced sexual imagery' best describes the practice because:

- 'Youth produced' includes young people sharing images that they, or another young person, have created of themselves.
- 'Sexual' is clearer than 'indecent.' A judgement of whether something is 'decent' is both a value judgement and dependent on context.
- 'Imagery' covers both still photos and moving videos

The types of incidents which can be regarded as youth produced sexual imagery are:

- A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18
- A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult
- A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18

College response to incidents involving 'youth produced sexual imagery':

The National Police Chiefs Council (NPCC) has made clear that incidents involving youth produced sexual imagery should primarily be treated as safeguarding issues. The College will therefore seek advice from the Child Protection Service for Schools on assessing the risks to the student(s) involved and if these can be managed within the College's pastoral support and Code of Conduct and if appropriate, the local network of support agencies.

Parents (or carers) will be informed and involved in the process at an early stage unless informing the parents/carers will put the young person at risk of harm. Any decision not to inform the parent/carers would generally be made in conjunction with other services such as the CPSS, Social Services and/or the PSNI, who would take the lead in deciding when the parents/carers should be informed. See the Child Protection Policy for the College response to incidents of 'youth produced sexual imagery'.

The following does not come within this classification of 'youth produced sexual imagery':

- The sharing of sexual imagery of people under 18 by adults as this constitutes child sexual abuse and the PSNI will always be informed.
- Young people under the age of 18 sharing adult pornography or exchanging sexual texts which do not contain imagery – such cases will be dealt with under the Code of Conduct.

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 located 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.

Students wishing to use their own device to access the C2k wireless network must first register their device with the ICT Technician.

Securus

Securus software alerts staff to any words on our network that would lead us to believe that our very high standards of safeguarding, reflected in our Acceptable Use Policy, might be being jeopardised. Securus is effective both online and offline across all programmes used by the College. Incidents flagged by Securus would include any evidence of bullying, inappropriate language, indicators of emotional distress and searches for harmful websites.

A screen 'capture' is taken of every incident, showing what was displayed at the time, who was involved and when the incident took place. These captures enable staff to respond promptly to situations which are potentially serious or in breach of the Acceptable Use Policy (AUP). The immediacy of this system can help prevent issues from developing into something more serious.

The use of this software complements our Online Safety curriculum to ensure that students are educated in using all aspects of ICT in a safe and responsible manner.

C2k filtering

Staff and students accessing the Internet in school via C2k Education Network will be required to authenticate using their C2k username and password which should never be shared. This authentication will provide Internet filtering via the C2k Education Network Solution. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the Principal.

Reporting

Students are made aware through assemblies who to report to if they have any concern about their on line safety. This information is also contained within the student homework diary. Staff report all instances relating to child protection to the designated teacher.

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 online 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 is 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 as soon as possible 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, social media or blog, particularly in association with photographs.
- The data capture form completed by the parents/carers of students enrolling in Portadown College requires parents/carers to state whether or not they grant permission for photographs of their child to be published on the College website, blogs, social media or other on line media used by the College.

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/carers (email, chat, VLE etc) must be professional in tone and content. Please see Netiquette guide (**Appendix 1**)
- The sending and receiving of e-mail communication with parents/carers must always be directed through the College info account: info@pc.portadown.ni.sch.uk
- Student names must 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's use of social media for professional purposes will be checked by the SLT to ensure compliance with the Online Safety Policy.

Staff use of personal devices

Personally owned mobile phones devices must be switched off or switched to 'silent' mode when in the classroom.
Bluetooth communication must be 'hidden' or switched off and mobile phones or personally-owned devices must not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and should only use work-provided equipment for this purpose. In exceptional circumstances when this is deemed necessary, all images must be transferred to a

C2k/school network storage area or College device ASAP and all images permanently removed/deleted from the personal device (including the 'deleted folder/trashbox' etc' if one exists).

If a member of staff breaches the College policy, then disciplinary action may be taken.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents/carers, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and conceal (**by inputting 141**) their own mobile number for confidentiality purposes.

Storage of Data

Staff must ensure that they:

- At all times take care to ensure the safe keeping and confidentiality 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" or locked (password protected) at the end of any session in which they are using personal data.
- Delete any data which has been downloaded onto a third party device e.g. home laptop from the school C2k storage provision. Once deleted, any such data file must also be deleted from the 'trash box'/deleted files folder on the device.
- Never leave a computer logged on unattended.
- 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.
- Do not view confidential files/information when their computer is connected to an interactive whiteboard or any other device which would allow others to view the information.

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
- the data must be securely deleted from the device, in line with College policy once it has been transferred or its use is complete.

The C2k Manager operates a Register of Access which outlines who has access to student and staff data on the school C2k system.

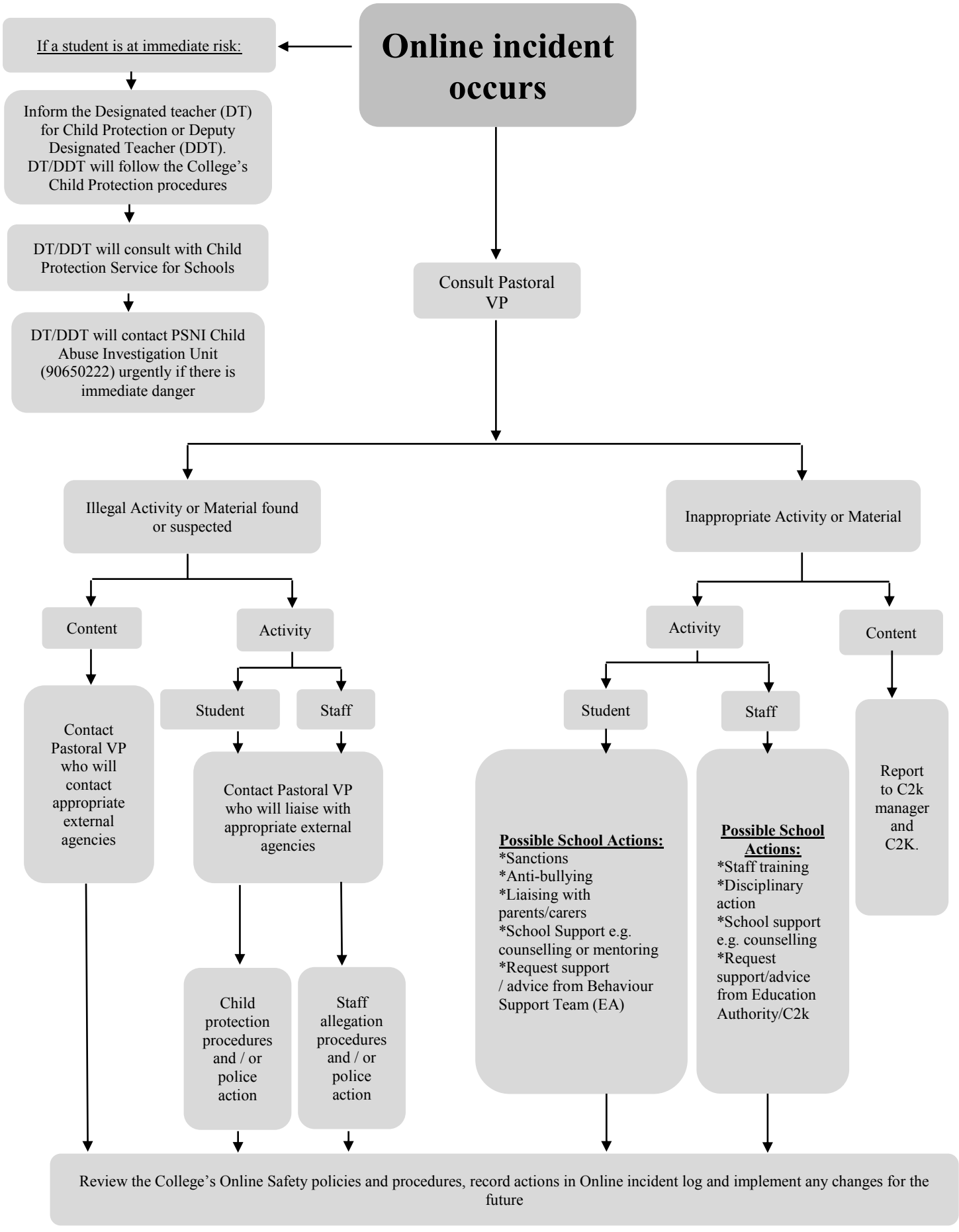
CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety and behaviour management. We will not reveal any recordings without permission except where requested by the Police as part of a criminal investigation.
We do not reveal any such recordings outside of the staff immediately involved and will not use these for any other purposes.

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 left hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.

Response to an Incident of Concern



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 College and 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/carers. In the event of illegal activities, this will involve referral to the PSNI.

Monitoring and Evaluation of this Policy

As part of the College Safeguarding procedures, an Online Safety Risk register is kept on file. This includes incidents recorded by the SECURUS software.

This Online safety policy has been reviewed by the Online 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, 2015/21 and 2016/26 when creating this policy.

The College uses the 360 degree safe on line tool to audit all aspects of online safety provision in the College.

The Online 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 online safety or incidents that have taken place. The next anticipated review date will be in **June 2019**.

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 (Info for Parents – Documents about PC)

This Policy was approved by the Board of Governors on 14 October 2014**.**
The updated Policy was approved by the Board of Governors on14 June 2018.

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

Appendix 2 – Reporting Log

	Action taken	By whom?			
		What?			
	Incident Reported by				
	Incident				
	Time				
	Date				

Appendix 3 – 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 Summary of Roles and Responsibilities

Governors	Responsible for the approval of the Online 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 online safety) of members of the College community The 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 online safety incidents)
Pastoral Vice Principal (Designated Teacher for Child Protection)	• leads the Online Safety committee • takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the College Online Safety policies/documents • ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place. • provides training and advice for staff • receives reports of online safety incidents and creates a log of incidents to inform future online safety developments • uses 360 on line tool to audit online safety provision each year • Helps parents understand these issues through parents' evenings, letters, website and information about national/local online safety campaigns
C2k/Capita	Is responsible for ensuring that: • the College's *C2k* technical infrastructure is secure and is not open to misuse or malicious attack
C2k Manager (curriculum)	Is responsible for ensuring that: • the College meets online safety requirements and any C2k or other relevant body (e.g. EA S Region) Online Safety Policy / Guidance that may apply. • users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. • the Register of Access is reviewed and updated on a regular basis • A record is kept at all times of current, legacy and intermittent staff users of College networks
ICT Co-ordinator	• Promotes key online safety messages across the curriculum and through special events e.g. Internet Safety Day • Assists the Pastoral Team in the creation of a co-ordinated Online Safety Curriculum strand of the PD programme
Year Heads	• Engage in the planning and review of the PD curriculum with the Pastoral VP and ICT Co-ordinator • Implement and evaluate the College's Online Safety curriculum as part of the PD programme
ICT Technician	• Ensures the College' technical infrastructure (outside that provided by C2k) is secure and is not open to misuse or malicious attack • Liaises with the C2k manager (curriculum) to ensure e-mail groups and access groups are monitored and updated when staff changes occur • Monitors SECURUS reports on a daily basis and passes on any concerns to the Safeguarding Team • Deals with any student issues relating to password security
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 College Online 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 Principal for 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) including how to report a concern. • 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 College digital 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 online safety practice when using digital technologies out of school and realise that the College's Online 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/ Carers	Parents and carers will be encouraged to support the College in promoting good online 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

Appendix 5 – Resources

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

- www.thinkuknow.co.uk
  An education initiative by the Child Exploitation and Online Protection (CEOP) Centre

- 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/carers make informed choices about their children's online safety.

- 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.

Appendix 6 – Acceptable Use Policies

Fortiter et Humaniter

Acceptable Use of ICT: Staff and Volunteer Policy Agreement

Rationale
Portadown College recognises that new technologies have become integral to the lives of adults and young people in today's society, both within and outside educational contexts. These technologies can promote effective learning and facilitate effective communications.

At Portadown College we believe staff (teaching/non-teaching and, where applicable, volunteers) should have good access to ICT to enhance the learning experiences of students and their own professional development. In return, Portadown College expects staff and volunteers to be professional and responsible in their use of ICT. It is Portadown College's expectation that, where possible, staff (and volunteers) educate students in the safe use of ICT, embedding e-safety in their work and demonstrating professionalism in their own ICT use.

As a Member of Staff/Volunteer:

- I understand that Portadown College and C2k will monitor my use of the ICT systems, email and other digital communications.
- I will follow the guidelines set out in **Portadown College's Child Protection Code of Conduct for Staff and Online Safety Policy**.
- When using e-mail to communicate with students and parents/carers I will only use the official school system.
- I will ensure the contents line of any e-mail communication does not contain student names to ensure confidentiality where e-mail may pop up on whiteboard screens being used in classrooms.
- If using other forms of on line communication, I will conform to the guidance set out in the Online Safety policy.
- I will ensure that when I take and/or publish images of others, I will do so in accordance with Portadown College's Child Protection Code of Conduct for Staff.
- I will not disclose my username and/or password to anyone else, nor will I try to use any other person's username and password.
- I will report immediately any illegal, inappropriate or harmful material or incident of which I am aware to the VP (Pastoral).
- I will communicate digitally/electronically with others in a professional manner and will not engage in any activity that may compromise my professional responsibilities.
- I understand that data protection policy requires that any staff or student data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or College policy to disclose such information to an appropriate authority.
- I will not download or distribute copies (including music and videos) in cases where work is protected by copyright.
- I will not upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others.
- I will not disable or cause any damage to College equipment, or equipment belonging to others.

- I will not open any hyperlinks in emails, or any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not allow any student to use my allocated school iPAD if I have installed the SIMs app to access student data (take the register etc).
- I understand that the Principal or appointed Senior Staff can request an Internet Usage Report for any member of staff using the core C2k EnNi service.

- I am aware that if using *Google Apps for Education* (GAFE - available through Fronter) I must abide by the terms and conditions of the Online Agreement and the College AUP. I understand that:

- As with any cloud based storage it may be unavailable at certain times or that **data could be lost** and therefore I should always back up my work on the C2k network.
- No confidential information should be stored in GAFE as the security of this on line provision cannot be guaranteed.
- I should only use GAFE for school business.

I have read the above and understand that:

(i) All of the above apply to my use of College ICT systems (eg. desktops, laptops, email, VLE) both inside and outside school.
(ii) When I use personal mobile devices (eg. PDAs, laptops, mobile phones, USB devices) in College, I must adhere to the above in the same way as when using school equipment and systems.

Staff/Volunteer Name: _____

Signed: _____ **Date: _____**

Fortiter et Humaniter

Acceptable Use of ICT: Student Policy Agreement

Rationale

Portadown College recognises that new technologies have become integral to the lives of young people in today's society, both within and outside school. These technologies can stimulate creativity and promote effective learning.

At Portadown College we believe students should have an entitlement to safe internet access at all times. Portadown College will endeavour to ensure that students have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Aims

This Acceptable Use of ICT Student Policy is therefore intended to ensure:

- that students are responsible users and stay safe while using the internet and other communications technologies for educational purposes in College;
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

<u>As a College Student:</u>

- I understand that I must use the school ICT systems (including Wi-Fi access) in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I understand that the school ICT systems are intended for educational use and I will not use the systems for personal or recreational use.
- I understand that Portadown College and C2k will monitor my use of the school ICT systems (including Wi-Fi access), email and other digital communications.
- I understand the risks and will not upload, download or access any materials which are illegal and/or inappropriate, obscene or abusive, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not share my username and/or password, nor will I try to use any other person's username and/or password.
- I will ensure that I lock my workstation if I need to leave it unattended
- I will not disclose or share personal information about myself or others when online.
- I will be aware of the potential threats associated with communicating with strangers online.
- I will agree to adhere to the College's Code of Conduct with regard to use of personal handheld/external devices (e.g. mobile phones/ipods/USB devices, cameras, video cameras, ipads, tablets, laptops, netbooks) in school.
- I accept that this Agreement covers accessing the internet through any personal device I bring into the College
- I will not record and/or upload live footage of school activities or events inside or outside the classroom onto any video file sharing platforms (e.g. You Tube, Facebook and/or other social networking sites) without permission from a member of the teaching staff.
- I will not take or share images of any members of the school community without first requesting and receiving their consent.

- I will be respectful and responsible when I communicate with others using ICT.
- I will immediately report to a member of staff any inappropriate, obscene, abusive or illegal material or messages I receive though the C2k email or other official school electronic forms of communication.
- I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not, unless I have the permission of a member of staff, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will only communicate with staff on line through approved channels eg: C2k email or Fronter VLE and school social media accounts.
- I will not seek to befriend or follow any member of staff on any social media network.
- I will immediately report any damage or faults involving equipment or software to a member of staff.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will not interfere in anyway with ICT equipment being used by staff.
- I will recognise that copyright laws should not be broken when using the internet for research and will not plagiarise the work of others.
- I understand that the Principal or appointed Senior Staff can request an Internet Usage Report for any student using the core C2k service.
- I am aware that if using *Google Apps for Education* (GAFE - available through Fronter) I must abide by the terms and conditions of the Online Agreement and the College AUP. I understand that:
  - As with any cloud based storage it may be unavailable at certain times or that **data could be lost** and therefore I should always back up my work on the C2k network.
  - No confidential information should be stored in GAFE as the security of this on line provision cannot be guaranteed.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use of ICT Student Policy Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

PLEASE RETAIN THIS PART OF THE POLICY

PLEASE RETURN THIS PART OF THE POLICY

Portadown College Acceptable Use of ICT: Student Policy Agreement Form

This form relates to the **Portadown College Acceptable Use of ICT: Student Policy Agreement** which is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in **Acceptable Use of ICT: Student Policy Agreement**. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I understand that it is my responsibility to use ICT appropriately, both in and out of school:

- I understand that Portadown College has the right to impose sanctions if I use ICT inappropriately, both in and out of school, in a manner which discredits Portadown College or members of the Portadown College community.
- I understand that if I fail to comply with this **Acceptable Use of ICT Student Policy Agreement**, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents/carers and, in the event of illegal activities, involvement of the PSNI.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school). This includes the VLE and Google Apps for Education.
- I use my own equipment in school (when allowed) e.g. mobile phones/ipods/USB devices, cameras, video cameras, ipads, tablets, laptops, netbooks.

I understand that Portadown College accepts no responsibility for the safety of students' personal equipment.

Name of Student: _____

Year Group: _____ Registration Group: _____

Signed: _____ Date: _____

PR/June 2017