PENRYN COLLEGE

E- SAFETY POLICY

At Penryn College we recognise that the Internet and new technologies provides a vast opportunity for young people to enhance their learning in new and exciting ways. However, these opportunities should also be explored alongside a sound understanding of the risks that young people might face.

Approved by: Full Governing Body – December 2016

Responsible SLT member: John Harvey

To be reviewed: October 2017

Published: Virtual School, Website, Staff Handbook

Contents

Appendices:

PENRYN COLLEGE - E-SAFETY POLICY

This policy has been developed by a working group made up of:

- ✓ *School E-Safety Officer (Designated Safeguarding Lead)*
- ✓ *Senior Leaders*
- ✓ *Teachers*
- ✓ *Administration Staff*
- ✓ *ICT Technical staff*

Consultation has taken place through the following:

- ✓ *E-Safety Sub-committee meeting*
- ✓ *Parents Forum*
- ✓ *School Council (Student Acceptable Use Policy)*
- ✓ *SLT*
- ✓ *Student E-safety group*
- ✓ *Governors' Safeguarding Scrutiny Committee*

Schedule for Monitoring, Review and Development

This E-safety policy was approved by the Full Governing Body on*:*	8th December 2016
The implementation of this e-safety policy will be monitored by the:	E-Safety Committee
Monitoring will take place at regular intervals:	Annually
The Student and Curriculum Committee will receive a report on the implementation of the E-safety policy generated by the monitoring group (which will include anonymous details of E-safety incidents) at regular intervals:	Annually
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:	October 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, Police Commissioner's Office

The school will monitor the impact of the policy throughout the year using:

- ✓ Logs of reported incidents
- ✓ SWGfL monitoring logs of internet activity (including sites visited)
- ✓ Internal monitoring data for network activity
- ✓ Monitoring of Filtering protocols and logs of reported incidents by E-safety Governor every Half Term
- ✓ Surveys / questionnaires/Governor Focus Groups of :
  - students / pupils (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey) - parents / carers
  - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

The policy will also reflect the recommended practice and priorities as set out in , including 'Keeping Children Safe in Education September 2016'

Roles and Responsibilities

Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. There is a nominated E-Safety Governor **(Mark Parsons)** who will meet regularly with the E-Safety Co-ordinator / Officer to review e-safety incident logs, filtering/change control logs and report annually to the Governors Curriculum and Personnel Committee.

Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ESafety Officer.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive monitoring reports from the E-Safety Officer twice a year.
- The Headteacher and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff**.** (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant HR disciplinary procedures)

E-Safety Officer (John Harvey):

- ✓ leads the E-safety Committee
- ✓ takes day to day responsibility for e-safety issues and has a leads in establishing and reviewing the school e-safety policies / documents
- ✓ ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- ✓ ensures the Staff Development Co-ordinator provides training and advice for staff
- ✓ liaises with external agencies as appropriate
- ✓ liaises with school ICT technical staff
- ✓ receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- ✓ meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- ✓ attends relevant meeting of Governors
- ✓ reports regularly to Senior Leadership Team
- ✓ ensures that national and local priorities, and advice and guidance, such as that detailed in 'Keeping Children safe in Education September 2016', are dissimated to the E-safety Committee and all staff.
- ✓ ensures that the school curriculum and Assembly programme addresses national and local E-safety priorities effectively

Network Manager / Technical staff:

The Network Manager and ICT Technical Staff are responsible for ensuring:

- ✓ the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- ✓ the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any other relevant E-Safety Policy and guidance, including 'Keeping Children Safe in Education September 2016'

- ✓ users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- ✓ SWGfL is informed of issues relating to the filtering applied by the Grid
- ✓ the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- ✓ that the Network Manager keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- ✓ the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the system administrator for investigation, action and if necessary refer to E-Safety Officer for sanction
- ✓ monitoring systems are implemented and updated as agreed in school policies

Teaching and Support Staff are responsible for ensuring:

- ✓ they have an up to date awareness of e-safety matters and have read and understand the current school e-safety policy and practices
- ✓ they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- ✓ they report any suspected misuse or problem to the system administrator for investigation / action and, if appropriate sanction
- ✓ digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- ✓ e-safety issues are embedded in all aspects of the curriculum and other school activities
- ✓ pupils understand and follow the school e-safety and acceptable use policy
- ✓ pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ✓ they monitor ICT activity in lessons, extra curricular and extended school activities
- ✓ they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- ✓ in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

The Designated safeguarding Lead (DSL) is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming, including the dangers of Child Sexual Exploitation
- cyber-bullying, including 'Peer on Peer' abuse
- Radicalisation

E-Safety Committee (E-Safety Co-ordinator (DSL), System Administrator, Deputy Safeguarding Lead and nominated governor):

Members of the E-safety Committee will assist the E-Safety Officer with:

- ✓ the production, review and monitoring of the school e-safety policy / documents and - ✓ the school filtering policy

Students:

- ✓ are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy and the I-Pad Acceptable Use Policy, which they will be expected to sign before being given access to school systems and their I-Pad.
- ✓ 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, whether by adults or 'Peer on Peer' abuse, misuse or access to inappropriate materials and know how to do so
- ✓ will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying. Students should also understand the consequences of breaking any such policies.
- ✓ should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents:

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children. We will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national and/or local e-safety campaigns and literature. Parents and carers are responsible for:

- ✓ endorsing (by signature) the Student / Pupil Acceptable Use Policy/I-Pad Acceptable Use Policy
- ✓ accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users:

Community Users who access school ICT systems as part of the Extended School provision are expected to sign a Community User AUP before being provided with access to school systems. All visitor users of the school ICT system, will do so as members of staff for a day and will be subject to the same user agreement as members of staff.

Policy Statements

Education – students:

The education of students in e-safety is an essential part of the school's e-safety provision. Students need the help and support of the school to recognise and avoid e-safety risks and build their resilience in the use of the internet and new technologies.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities, including the risks of CSE and Radicalisation
- Students should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Where there is evidence that students have used social media or e-mail to abuse another student, the school will address this behaviour through restorative justice in addition to other appropriate sanctions detailed in the Behaviour Policy sanctions. Furthermore, as a school, where we believe criminal behaviour has been undertaken, will recommend the victims of any 'hate crime' or criminal misuse of social media, to contact the police prior to any school investigation taking place.'
- Annually we have an afternoon where we 'collapse' the timetable and deliver an E-safety lesson to all students.

Education – parents / carers:

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents evenings and Parents' Forum events
- Reference to E-safety websites

Education - Extended Schools:

The school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be delivered to staff. An audit of the esafety training needs of all staff will be carried out regularly
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Officer will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff /team meetings and/or INSET days. This will include raising awareness of the risks to students from CSE, 'Peer on Peer' abuse, and radicalisation
- The E-Safety Officer (or other nominated person) will provide advice, guidance and training to individuals as required

Training – Governors:

Governors should take part in e-safety training and/or awareness sessions, with particular importance for those who are members of any sub committee or group involved in ICT, e-safety, health and safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association, SWGfL or other relevant organisation.
- Participation in school training and information sessions for staff or parents
- Updates at Governors' Safeguarding Scrutiny Meetings each Half Term

ALL GOVERNORS SHOULD ATTEND TRAINING IN RELATION TO THE PREVENT AGENDA.

Technical – infrastructure / equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems**.** Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee.
- All users will be provided with a username and password by the System Administrator who will keep an up to date record of users and their usernames. Users will be required to change their password if there has been any possibility of that password being compromised but users are expected to change passwords regularly as part of good e-safety practice.
- The "master administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL
- The school has provided enhanced user-level filtering through the use of the Smartcache filtering programme.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and E-Safety Officer. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity.
- An appropriate system is in place for users to report any actual or potential e-safety incident.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious activities which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices without consultation with the Network Manager.

- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations or portable devices.
- The school infrastructure and individual workstations are protected by up to date anti-virus software.
  Personal data may not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum:

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to independently search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should be taught in all lessons to be critically aware of the materials and 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.

Use of digital and video images - Photographic, Video:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils 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.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- ✓ Fairly and lawfully processed
- ✓ Processed for limited purposes
- ✓ Adequate, relevant and not excessive
- ✓ Accurate
- ✓ Kept no longer than is necessary
- ✓ Processed in accordance with the data subject's rights
- ✓ Secure
- ✓ Only transferred to others with adequate protection.

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 personal 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 and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- ✓ the data must be encrypted and 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.

Communications :

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks or disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not Allowed
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓				✓			
Taking photos on mobile phones or other camera devices	✓*					✓		
Use of hand held devices eg PDAs, PSPs	✓					✓		
Use of personal email addresses in school, or on school network				✓**				✓
Use of school email for personal emails	✓					✓		
Use of chat rooms / facilities	✓							✓
Use of instant messaging	✓					✓		
Use of social networking sites				✓				✓
Use of blogs	✓					✓		

* These images should only be taken on school equipment

**Unless under exceptional circumstances and agreed with the Network Manager and the E-Safety Officer

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

- ✓ The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when conducting school business
- ✓ Users need to be aware that email communications may be monitored
- ✓ Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- ✓ Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- ✓ Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- ✓ Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities:

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyberbullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓

	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)			✓			
On-line gaming (non educational)			✓			

On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing in accordance with Penryn College's policies	✓				
Use of social networking sites			✓		
Use of video broadcasting eg Youtube			✓		

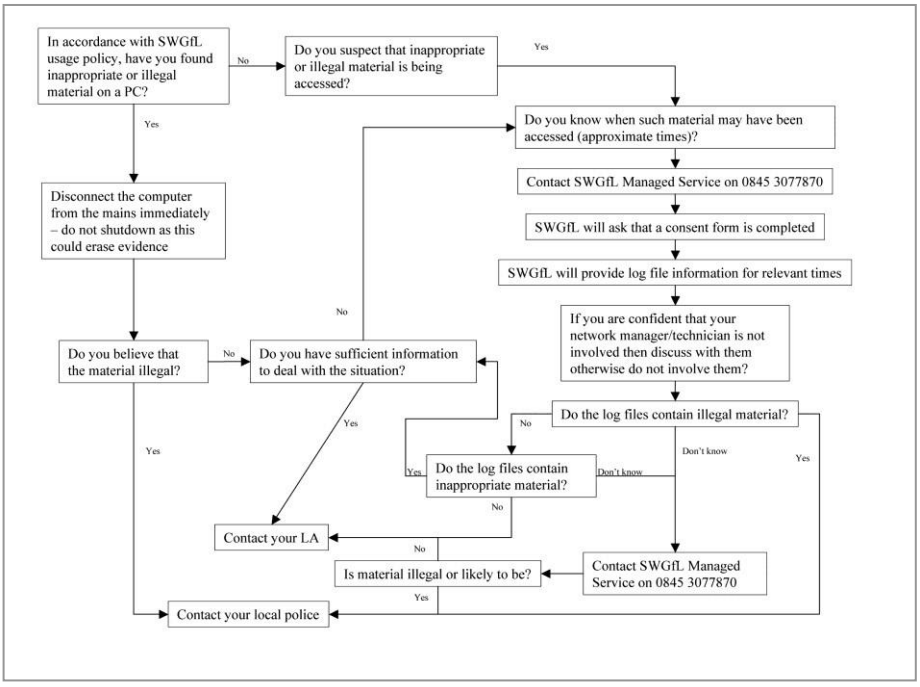
Responding to incidents of misuse:

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The SWGfL flow chart – below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Sanctions

For Students:

Level 1:

- Pupil is given a verbal reprimand by Class Teacher/ tutor and the incident is logged on Behaviour Manager
- Repeated offences will result in meeting with a Senior Leader and the E-Safety Officer and the incident will be logged.
- Letter will be sent to parents/guardians informing them of the incident and reminding them of the Student Acceptable Use Policy.
- Head of House informed.
- Three or more offences will escalate to level 2 sanction.

Level 2:

- Letter is sent to parents/guardians informing them of the incident and reminding them of the Student Acceptable Use Policy. Head of House informed.
- Repeated offence – Parent is requested to attend meeting to resign the Student AUP.
- Three or more offences Headteacher notified and will escalate to level 3 sanction.

Level 3:

- If a criminal activity is involved then the matter will be referred to the Police.
- If the activity is not illegal the Headteacher is consulted and action will be taken on a case to case basis but may involve detention/removal of email access/removal of internet access rights and/or exclusion.

For staff

Level 1:

- Member of staff is given a verbal reminder (and reprimand if appropriate) by the Headteacher or SLT link and the incident is logged on their personnel file and also logged on E-Safety file. Repeated offences will be reported to Headteacher

Level 2:

- Letter from Headteacher is sent to member of staff reminding them of AUP and a copy of the letter is placed on their Personnel file.

Level 3

- Breaches at this level could result in a suspension/referral to Governors and in the event of illegal activities, the involvement of the police.

Students:

Incidents:	Level 1	Level 2	Level 3
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	
Unauthorised use of non-educational sites during lessons	✓		
Unauthorised use of mobile phone / digital camera / other handheld device (see also Mobile Phone Policy)	✓		
Unauthorised use of social networking / instant messaging / personal email		✓	
Unauthorised downloading or uploading of files		✓	
Allowing others to access school network by sharing username and passwords		✓	
Attempting to access or accessing the school network, using another student's / pupil's account		✓	
Attempting to access or accessing the school network, using the account of a member of staff		✓	
Corrupting or destroying the data of other users		✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓
Continued infringements of the above, following previous warnings or sanctions			✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	

Using proxy sites or other means to subvert the school's filtering system		✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	
Deliberately accessing or trying to access offensive or pornographic material		✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓

Staff:

Incidents:	Level 1	Level 2	Level 3
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓	
Unauthorised downloading or uploading of files		✓	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓	
Careless use of personal data eg holding or transferring data in an insecure manner			✓
Deliberate actions to breach data protection or network security rules			✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓
Using **personal** email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✓	✓

Actions which could compromise the staff member's professional standing	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓
Using proxy sites or other means to subvert the school's filtering system		✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	
Deliberately accessing or trying to access offensive or pornographic material			✓
Breaching copyright or licensing regulations			✓
Continued infringements of the above, following previous warnings or sanctions			✓

Appendix 1: Parent/ Carer AUP

PARENT/CARER ACCEPTABLE USE POLICY

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Penryn College will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. Please read the Student Acceptable Use Policy e so that you are aware of the school's expectations of your child while in our care.

Parents/Carers are requested to sign below to show your support of the School in this important aspect of our work.

Parent/Carers Name _____

Student/Pupil Name _____

As the parent/carer of the above pupil, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed _____Date _____

Appendix 2:

PENRYN COLLEGE – STAFF AND VOLUNTEER COMPUTER RESOURCES ACCEPTABLE USE POLICY

Introduction

New technologies are integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe internet access at all times.

The standard signature that goes out automatically on all emails from the College includes the following "If the contents of this email are not Penryn College business then in sending this email the sender is not acting as an agent, representative, or in any other capacity for or on behalf of Penryn College. Penryn College accepts no responsibility whatsoever and howsoever arising in connection with this e-mail."

This Acceptable Use Policy is intended to ensure that:

- staff and volunteers are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that there is good access to ICT to enhance work and learning opportunities for all. We expect staff and volunteers to agree to be responsible users.

ACCEPTABLE USE POLICY AGREEMENT

I understand that I must use School ICT systems 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 recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will ensure that e-safety is paramount in my work using new Technologies .

For my professional and personal safety:

- I understand that the school monitors my use of the ICT systems, email and other digital communications;
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school;
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by this policy.

- I will not disclose my username or password to anyone else, and will not try to use any other person's username and password;
- I will immediately report any illegal, inappropriate or harmful material, including emails of a sexual or racist nature, or incident, I become aware of, to the Network Manager/ Network Support Team;
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission;
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. Training will be provided in acceptable email protocols;
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. If these images are published electronically it will not be possible to identify subjects unless this has been sanctioned'
- I will ensure that any photographs I take do not include subjects that I do not have permission to photograph, particularly with regard to children in the background. I will not publish any such photographs unless I have permission to do so for all subjects.
- I will not use any chat or social networking sites in school for example Facebook, Bebo and MySpace and I will not befriend pupils in or out of school.
- I will only communicate with students, parents and carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- If leaving my pc for some time I will make sure I lock it to secure my documents.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

- If I want to use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) on the school network, or with school equipment , I will need the prior agreement of the network support staff and I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not allow any personal devices (PDAs/laptops/mobile phones/USB devices etc) to be used by pupils. Any equipment shortfall will be referred to the ICT technical staff for assistance.
- I will not open 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 try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) and I understand that all incidents will be reported to the Police and I will be suspended from my post pending investigation.

- I will not try to upload, download or access any materials which are inappropriate or may cause harm or distress to others;
- I will not 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 try (unless by prior arrangement with the Network Manager) to 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 not copy, install or attempt to install programmes of any type on or from a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies;
- I will not disable or cause any damage to school equipment, or the equipment belonging to others;
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Act 1998. Where personal data is transferred outside the secure school network, I understand that it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it s deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority;
  - I will immediately report any damage or faults involving equipment or software.

When using the network/ internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school and that

- This Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my personal equipment in school or in situations related to my employment by school;
- If I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and /or the Local Authority and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Student teacher/Volunteer Name ___ _____

Signed _____ Date _____

Appendix 3:

PENRYN COLLEGE – STUDENT ACCEPTABLE USE POLICY

Information Communication Technology (I.C.T) is one of the core subjects that make up the National Curriculum, and as such, forms an important part of your education. In fact ICT is increasingly used in all subjects.

In particular we hope you will find the schools' network useful for:

- carrying out research for projects
- finding images to illustrate your work
- doing homework
- creating imaginative and engaging PowerPoint's
- communicating with staff and pupils through email: each student will be given their own email account for school use.
- organising your time through the electronic calendar
- accessing the many information resources, including the internet

The school has invested in providing a 'state of the art' computer network so that all students at have the opportunity to use ICT to help them study.

It is important therefore, that the school network, software, user files and all associated equipment be used properly and treated carefully. It is also important that you do not upset or offend any other students or staff by sending or posting inappropriate material via email, mobile phone or on social networking sites. Please read this agreement and sign below to show you agree to abide by its rules. This will allow our network and resources to be maintained at the highest quality.

AGREEMENT

I agree:-

- during lesson times to use the school internet/intranet only as directed by my teacher. At all other times (breaks and lunchtime eg) I will only use them within the framework of school rules and policies.

- not to use the school internet to download or post **anything of an offensive nature to only send emails that are polite and respectful and to ensure that I never use internet or emails to bully or hurt others**
- to do **all I can to help look after** the school computers, including not drinking near PCs or interfering with equipment
- to cooperate with computer room staff during lunchtime clubs
- **to only access my user area and not to give my password to others**
- to check with teachers if I am unsure about what hardware I can bring in and use on the network (MP3s and 4s, mobile phones, handheld consoles and any other similar devices are **not** part of the school network and should **not** be connected to it)
- not to install **any** programmes or applications onto any school computer
- to access only areas of the network for which I have permission
- not to place copyrighted materials on to the school network
- to only use the software made available to me via the normal user desktops not to copy **any software** that exists on any of the schools' computers.

If in doubt ask an ICT teacher or ICT technician.

I understand that if I break this agreement, it could result in me not being allowed to use school computer facilities, disciplinary action being taken and may result in expulsion.

Pupil name _____

Signed _____ Date _____

Appendix 4:

Penryn College: Acceptable Use Policy for Mobile Digital Devices including iPads

September 2015 **Date of Review: May 2016**

Introduction

Penryn College may grant a licence to use iPads or other mobile digital devices (together referred to as "iPads" in this policy) to staff and students for the purpose of promoting educational excellence by offering access to information and tools that enhance learning, innovation, research, creativity, communication and enable mobile learning. This policy outlines the acceptable use of iPads and is supplementary to the college's other Acceptable Use Policies for ICT. IPads are a **privilege that carry responsibility** and behavioural expectations consistent with all college rules and policies [Behaviour Policy, Acceptable Use Policy for ICT]. IPads are provided and maintained for the benefit of the whole college community and students are encouraged to use and enjoy these resources, and to help ensure they remain available to all. Inappropriate use may result in disciplinary action.

Students are expected to have regard to this policy at all times to protect the iPads from unauthorised access and damage.

Scope

This policy applies to all students attending the college. All parents/ carers signing this policy on behalf of students agree that they (parents/ carers) have overall responsibility for ensuring safe and appropriate use of iPads and compliance with this policy. This includes responsibility for the use of iPads through internet connections at the student's home, or at a site other than the college.

Equipment

1. Each iPad will be restricted to a set of allowable Apps. The college will decide which Apps are made available and will be advised by student iPad Champions on future Apps to be added to the approved list.
2. No action will be taken that damages, disables or harms the operation of the iPad. The iPad will be kept away from liquids, heat and protected at all times by suitable screen protection and the supplied case.
3. The iPad will be used for the purpose of accessing information and as a tool to enhance learning. During lessons, iPads must only be used as, and when directed by, a member of staff. Use at break times is only permitted in designated areas of the school.
4. IPads must remain free of writing, drawing, stickers, labels or skins, unless provided or authorised by the college.
5. For use outside the college, it is the responsibility of parents/ carers to provide access to an appropriate internet connection. The iPad configuration will cause all connections to be routed via the college internet filter and will log websites accessed by each device.
6. While in the college, students will be provided with filtered, secure internet access. The college's network is the only internet connection that students will use whilst in the college.

7. The college reserves the right to inspect the iPads at any time to ensure that they are being used in accordance with this policy. There is no right to privacy for any files, email, social network, or any other content stored or accessed using an iPad.
8. The iPad will, at all times, remain the property of the college. The college reserves the right to recall the iPad or confiscate the iPad at any time and alter, add or delete installed software or hardware.
9. IPads must be brought to college each day, fully charged. IPads must be charged overnight in a secure place. Students must not bring mains chargers and cables into school as these are not PAT tested.

Security and Privacy

1. Passwords/ pin codes will not be shared except with parents and will be changed as directed by the college. Parents/ guardians should be able to access the machine for the purpose of supervising and supporting their child's learning.
2. Students must only use their own iPad. Students must not ask for another student's pin code/ password.
3. Students will not attempt to bypass the college's internet filtering. To do so is a breach of this policy and will be treated as a very serious behaviour incident.
4. There is no right to privacy when using an iPad. All files, emails, photos etc can be sampled by the college to ensure that the device is being used in an appropriate way. There will be a routine random audit process and if asked, students must make their iPad available immediately for sampling.
5. All iPads must have a lock code (password) enabled. The iPad will be set so that the lock activates automatically after a short period of time (e.g. 5 minutes). This will be controlled by the college.
6. IPads must never be left unattended in a public place, either on college premises or elsewhere. Nor should the iPad be left in plain sight within a vehicle. Lockers are available in college for students to store their iPads and other valuables.
7. In the event that the iPad is lost, damaged or stolen, this must be reported to the college immediately. If the iPad is broken or damaged, it must be taken immediately to the IT team for an evaluation. If the iPad is lost or stolen, police must be notified and the incident number reported to the college along with other reasonable details. There may be a £50 charge payable by parents towards replacement or repair costs should the iPad be damaged, lost or stolen as a result of recklessness or negligence. On a subsequent occasion of loss, theft or damage, this charge may increase.

Use of the Internet

1. The internet is available to students for educational purposes and whilst at the college, should be used by students for learning and educational activities.
2. Students should only access, and should only attempt to access, suitable learning material. Using the internet to obtain, download, send, print, display or otherwise transmit or gain access to

materials that are unlawful, obscene, or abusive is not permitted and will be treated as a serious behaviour incident.

3. The college will contact appropriate authorities including the Police in the event of unlawful access to materials.
4. Access to materials must respect the work and ownership rights of people. This includes abiding by copyright laws.
5. Access to materials, webpages, files (documents or images) that are in anyway illegal, offensive, in bad taste or immoral will be in breach of this policy. As a general rule, if any person might reasonably be offended by the contents of a page then viewing it will be a breach of this policy and will be treated as a serious behaviour incident.
6. Please note, ALL internet access is routed via the college and is logged against each individual iPad.

Use of email

Students' use of email, including on the iPads, is covered by the AUP all students sign before using the school network.

Use of social media

1. Initially the college iPads will not be able to access social media. In future, students will not be permitted to use the machines for this purpose unless their tutor and parents agree that they have earned this privilege.
2. In general the use of email and messaging networks within lessons is permitted only where for learning and when directed and supervised by a member of staff. Students must uphold, at all times, the highest standards when communicating for the purposes of learning using the college's iPads. Any posts that harm the college's reputation will be regarded as serious disciplinary offences.

Use of music, games and digital images

1. Initially students may not download music and games. Students are not permitted to use the machines for this purpose unless their tutor and parents agree that they have earned this privilege.
2. The taking of photographs and video, and other digital images, using the college's iPads is permitted only for the purpose of enhancing learning.
3. Any images taken for the purpose of enhancing learning must only be used within the lesson and the lesson's activities as directed by the teacher.
4. At the end of the lesson or learning activity, digital images that are no longer needed must be deleted.
5. The use outside the college of digital images taken during lessons, including posting or uploading images onto the internet or social media, sites is expressly forbidden.

6. In general, the consent of parents to take images of students is requested annually by the college. Only images that have parental consent will be used by the college for the purpose of marketing or reporting.
7. The use of iPads to take photos or videos of students outside of lessons is strictly forbidden. Posting digital images of students onto the internet or social media sites is a serious breach of this policy and will result in disciplinary action.

Personal Use of iPads

The use of iPads outside college for personal activities is permitted, providing the student complies with this policy. All activities on the iPad will be subject to routine sampling and checking procedures. If a student becomes aware that another student is in breach of this policy they must notify the IT team or another member of staff immediately.

Return of iPads

If a student leaves the college for whatever reason, the iPad must be returned during the final week of attendance at the college. The college reserves the right to recall the iPads without notice. Failure to follow the terms of this policy may result in the iPad being recalled by the college. Failure to return the iPad may result in a theft report being filed with the local police department, which may lead to criminal prosecution or civil liability.

Costs

At the end of the academic year or when the student leaves the college, the iPad, case and charging lead will be returned to the college. Deliberate or reckless actions by students which result in damage, loss or theft may result in parents being asked to pay a charge or, when appropriate, the full cost of repair or replacement. Repeated loss, damage or theft may result in the iPad not being available to the student outside of the college or it being withdrawn altogether.

Monitoring

The college will monitor the use of email, social media sites, files, downloads and any other activity carried out on the iPad provided by the college. There is no right to privacy when using the iPad.

Changes to this policy

The college reserves the right to make changes to this policy from time to time. Any changes will be notified to students and parents. The policy will be reviewed at least annually.

This policy must be read carefully by parents and students. Use of the college's iPads must be in accordance with this policy and breaches may result in disciplinary action. Where appropriate, police or other outside agencies may be informed and/or other legal action taken. This policy applies to the use of digital devices (iPads) owned by the college*.*

Summary iPad Policy

The points below summarise the agreement between parent, students and the college regarding the provision of iPads for students. More information is in the full policy, available on our website.

1. I will report any loss, theft or damage to the iPad to the college immediately. In the case of theft or loss, I will also report this immediately to the Police and tell the college the incident number of this report. I understand that the iPad is insured by the college and that a charge of £50 may be made to parents in the case of loss, theft or damage to the iPad.
2. I will not use inappropriate, abusive or discourteous language when sending any electronic communications (e.g. email) or encourage others to use such language.
3. I will not use my iPad during break or lunchtime unless specifically asked to do so by a member of staff or in one of the identified areas for this purpose.
4. I will use my iPad in lessons in the way in which I am asked, and follow the instructions given by the teacher.
5. I understand that the iPad is provided for learning. Any work, files, apps, games, photos or videos on the iPad are stored at the college's discretion and I will remove them if asked to do so.
6. I will not post, or encourage others to post, photos, videos or other material relating to Penryn College onto Facebook or any other social network site or website.
7. I understand the college will take disciplinary action if I am involved in an online activity that damages the reputation of the college, its staff or other students.
8. I will never leave the iPad in an unsecured or unlocked place.
9. I will inform the IT team or a member of staff if I witness or am informed of a breach of this policy or any improper use of an iPad by another student**.**
10. I will charge the iPad each evening at home and bring it into college every day.
11. I will ensure that the iPad is always suitably covered by the provided case with screen protection.
12. I will not take any action that has the potential to damage the iPad or the iPad belonging to another student or member of staff.
13. I will return the iPad, case and charging lead to the college on request. I understand that the iPad and charging lead remain the property of the college.
14. I understand that the iPad is provided for the purpose of learning and education and I will use the iPad for this purpose. Any Apps installed other than for this purpose will be removed on request by the college.
15. I will protect the iPad with a pin code/ password. I will share this password only with my parents/ guardians and no-one else . I will share my code with them so they can access my iPad when they want to. I will not use or attempt to use the password of another student.
16. I understand that the use of the iPad will be monitored by the college and that there is no right to privacy when using the iPad. I understand that any activity carried out on the iPad may be monitored by the college.

17. I understand the college may take action against me if I am involved in incidents of inappropriate behaviour when I am out of school. Examples would include cyber-bullying, inappropriate use of images, damage to the iPad etc. The college will involve the police or other agencies if appropriate.

Signature of student: _____

Signature of parent/ carer: _____

Date: _____

Appendix: 5

Cyberbullying:

What advice can we give our students at Penryn College?

We recognise that the internet is an amazing resource and can be used in a number of positive ways. However, content posted online can be easily misunderstood by others and taken out of context. It is important our students, parents/careers, and our staff recognise the importance of students 'thinking before they post' and the need for them to respect their friends' and peers' thoughts and feelings online. As a school, we believe that what's considered morally right and wrong offline must also be thought of in the same way online, and treating others with respect on the internet is a good way to ensure that online situations are less likely to escalate into cyberbullying situations.

Staff at Penryn College should:

1. Understand the tools: be aware of the reporting mechanisms on different sites and services so we can support our students in making a report.
2. Discuss cyberbullying: be proactive in discussing cyberbullying with our students; how it occurs, why it occurs, and the consequences of such behaviour.
3. Know who to report to: ensure that all staff make students aware of who to go to at Penryn College if they have concerns about cyberbullying incidents.
4. Understand that cyberbullying can also manifest itself as 'Peer on Peer' abuse

Through Tutor Period, assemblies, Curriculum lessons we advise students to:

1. Don't reply: most of the time the bully is looking for a reaction when they're teasing or calling someone nasty names. We advise our students not to reply, if they do they're giving the bully exactly what they want.
2. Save the evidence: encourage students to save the evidence of any emails or text messages they receive. This is so they have something to show when they do report the cyberbullying.
3. Tell someone: encourage our students to tell a trusted adult if they are being cyberbullied, and to tell them as soon as they can in order to minimise their own upset or worry.

Appendix: 6

Sexting

At Penryn College we define sexting as 'sending a sexually explicit message'

We believe we have a responsibility to ensure that all our students are aware of the law with regard to 'sexting'. We will do this annually through whole school assemblies, tutor period, curriculum delivery, and where appropriate with individual students as part of our e-safety individual support programme.

The law states that if a young person under the age of 18 engages in 'sexting' by creating an explicit photo or video of themselves then they have potentially created an image of child abuse. By sending this content on to another person, they have distributed an image of child abuse. By receiving content of this kind from another young person, they are then in possession of an image of child abuse.

Through whole school assemblies, tutor period, curriculum delivery, and where appropriate with individual students as part of our e-safety individual support programme, it is important that we ensure our students are aware of the risks of 'sexting'.'

What other risks are there?

- **Reputation damage:** with young people connecting via a wide range of technologies and social media sites, sexting content can be distributed to other users very quickly. This prevents the young person from controlling where the content is posted. This can result in damage to a young person's reputation in their school or local community, and in online communities. As content posted online can potentially exist forever in the public domain, this can have longer term effects on a young person's reputation and aspirations.

- **Emotional and psychological damage:** the distribution of sexting content to others can cause distress and upset to the young person involved, especially if the content is distributed by someone they entrusted it to. The effects of others seeing this content can lead to negative comments and bullying, and may result in a young person losing confidence or self-esteem, and in extreme cases can lead to depression and other risks.

As staff we should always give the following advice in relation to 'sexting':

- **Resist peer pressure:** the creation of sexting content is quite often due to pressure from a partner or group. Discussing peer pressure with your pupils is a positive way to encourage them to take responsibility for their own actions and resist pressure from others to engage in activities they are uncomfortable with, or know to be against the law.
- **Know the law:** although pupils will be treated as victims in instances of sexting, it is important to educate them about how such behaviour breaks the law, and the potential consequences.
- **Understand the consequences:** increasing your pupils' awareness about what can happen after sexting content has left their control is very important in helping them to understand the effects that may have on their reputation and psychological wellbeing; both short term and long term.
- **Lose your inhibitions and you lose control:** the distribution of sexting content is often deliberate but can also happen in a less planned way, for example through spontaneity or peer pressure, or if a young person is under the influence of alcohol or drugs and their judgement is impaired. Remind your pupils that they have control over the images they create and share, but once they have shared that content, it is out of their control.

It's never too late to tell someone: encourage pupils to speak to someone they trust if they are involved in a sexting incident. Although it may feel like the end of the world to a young person, there is always a way back. The quicker they speak to someone, the better the chance of managing the spread of the content.

Appendix 7

Prevent – Protecting students from the risk of 'Radicalisation'

At Penryn College we are committed to promoting student welfare and safety. As part of this, we believe it is important to protect students from the risk of radicalisation. It is essential that our staff are able to identify students who may be vulnerable to radicalisation, and know what to do when they are identified.

However, this does not mean that we believe that our students shouldn't debate issues such as 'extremism'; on the contrary, we feel it is important that students are able to debate such controversial topics in the safety of the classroom and develop the knowledge and skills to be able to challenge extremist arguments. In conjunction with this, we also believe that the promotion of British Values, enable our students to build resilience to radicalisation.

All our Safeguarding staff and those who deliver our PSHEE curriculum have been trained in the **Channel Process**.

For further information see the Department for Education's guidance: **The Prevent duty Departmental advice for schools and childcare providers June 2015**

PREVENT – VULNERABILITY ASSESSMENT FRAMEWORK

Staff Should:
✓ Identify individuals at risk of being drawn into terrorism ✓ Assess the nature and extent of that risk ✓ Develop the most appropriate support plan for the individuals concerned

Risk Assessment:

Nature of Risk:	Level of risk (1-5)*
Engagement with a group, cause or ideology	
Feelings of grievance and injustice	
Feeling under threat	
A need for identity, meaning or belonging	
A desire for status	
A desire for excitement and adventure	
A need to dominate and control others	
Susceptible to indoctrination	
A desire for political or moral change	

Opportunistic involvement	
Family or friends involvement in extremism	
Being at a transitional time of life	
Being influenced or controlled by a group	
Relevant Mental Health issues	
Intent to cause harm	
Over-identification with a group or ideology	
'Them and us' thinking	
Dehumanisation of the enemy	
Attitudes that justify offending	
Harmful means to an end	
Harmful objectives	
Capability to cause harm	
Individual knowledge, skills and competencies	
Access to networks, funding or equipment	
Criminal capability	
Total	

*5 is the greatest level of risk

Action Taken:

Action Taken:		Date Action Completed:
Referral To Channel Process		
Referral to MARU		
Pastoral Support Plan		
Parents/Carers informed		
Staff informed		
No further Action		