PENRYN COLLEGE

Online Safety Policy

Approved by:	Full Governing Body
Date Approved:	<Month and Year>
Responsible SLT member:	Designated Safeguarding Lead
To be reviewed:	December 2026
Published:	Virtual School, Website, Staff Handbook
Version:	2025-03-19 Online Safety Policy v1.0 Draft

Online Safety Statement

Penryn College understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Contents

Appendices:

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with all relevant policies, including:

- Low-level Concerns Policy
- Acceptable Use Agreements
- Keeping Children Safe in Education Policy
- Anti-Bullying Policy
- PSHE Policy
- Relationships and Sex Education Policy
- Code of Conduct for Penryn College Staff
- Cyber Security Policy
- Data and Cyber Security Breach Management Plan (currently being drafted)
- Behaviour Policy
- Staff Disciplinary Policy
- Data Protection Policy
- Mobile Device Acceptable Use Policy (Appendix 4)
- Staff / Volunteer Acceptable Use Policy (Appendix 2)
- PREVENT Statement (Appendix 7)
- Student Acceptable Use Policy (Appendix 3)

2. 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 Online 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 Online Safety behaviours that take place out of school.

The policy will also reflect the recommended practices and priorities as set out in the policies referenced above, including 'Keeping Children Safe in Education September 2022'

3. Roles and Responsibilities

The **Governing Body** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.

- Ensuring their own knowledge of online safety issues is up-to-date. Governors should take part in Online Safety training and/or awareness sessions, with particular importance for those who are members of any sub-committee or group involved in ICT, Online 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 orother relevant organisations
    - 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
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The H**eadteacher** is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The **Designated Safeguarding Lead** is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.

- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the Governors Safeguarding Committee about online safety on a termly basis.
- Working with the headteacher and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

The **ICT Technicians** are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to create a half-termly report based on light touch reviews of this policy.

All **Staff members** are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

The Designated Safeguarding Lead is trained in Online 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

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 / Virtual School and information about national and / or local Online Safety campaigns and literature. Parents and carers are responsible for:

- endorsing (by signature) the Student Acceptable Use Policy / Mobile Device Acceptable Use Policy

- accessing the school website / Virtual School / 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 the Staff / Volunteer / Visitor 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.

4. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.
The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.
The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation

- Online safety is integrated into learning throughout the curriculum and Online Safety education will be provided in the following ways:
    - A planned Online Safety programme will 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 Online 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 criminalmisuse of social media, to contact the police prior to any school investigation taking place.'
    - Online Safety lessons are delivered through LifeSkills and STEAM every year to all students.
    - Assemblies are conducted annually on the topic of remaining safe online

Handling online safety concerns

- Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the

Keeping Children Safe in Education Policy.

- Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.
- Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.
- The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.
- Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.
- Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.
- Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Keeping Children safe in Education Policy.
- Where there is a concern that illegal activity has taken place, the headteacher contacts the police.
    - The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Keeping Children Safe in Education Policy.
- All online safety incidents and the school's response are recorded by the DSL.

5. Cyberbullying (see also Appendix 5: Addressing Cyberbullying)

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.
Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

6. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.
The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.
Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.
The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.
The school responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

7. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.
Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.
CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.
Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.
Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.
Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

8. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.
Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

9. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.
For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.
Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.
The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content

is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.
Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding (KCSIE) Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.
The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

10. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.
The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum as described in Section 4; however, it is particularly addressed in the following Lifeskills subjects:

- RSE
- Health education
- PSHE

And in our curriculum for

- Citizenship
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.
Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in **Appendix A** of this policy.
The DSL is involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.
The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.
The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.
Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.
Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.
During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.
If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Keeping Children Safe in Education Policy.
If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Keeping Children Safe in Education Policy.

12. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Virtual School environment
- Email
- Digital Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.
Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.
Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Student Acceptable Use and Mobile Device Policies.
Staff will use all smart technology and personal technology in line with the school's Staff Acceptable Use Policy.
The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.
Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use personal smart devices or any other personal technology whilst in the classroom.
Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.
Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.
The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.
The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.
The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted access to the school network in the Technical Support Office and HR Department.
All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

15. Network Security, Activity Monitoring and Content Filtering

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 whose roles are listed in the preceding sections will be

effective in carrying out their Online Safety responsibilities.

There will be regular reviews and audits of the safety and security of school ICT systems:

- Servers, wireless systems and cabling are securely located and physical access restricted
- All users have clearly defined access rights to school ICT systems**.** Details of the access rights available to groups of users will be recorded by the Technical Support team and will be reviewed annually by the Safeguarding Committee.
- All users will be provided with a username and password by the Technical Support team 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 staff users are obliged to change passwords every 6 months as part of good Online Safety practice and as dictated by the school's Cyber Security Policy. Passwords will meet the minimum specifications for password properties as laid out in the Cyber Security policy.
- All staff users will employ 'Two Factor Authentication' (2FA) as directed within the Cyber Security Policy
- The "master administrator" passwords for the school ICT systems, used by key Technical Support personnel must also be available to the Headteacher or other nominated Senior Leader and kept in a secure place (e.g. 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 an in-house managed filtering service
- The school has provided enhanced user-level filtering
- In the event of the Technical Support personnel 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 the Technical Support team.
- Requests from staff for sites to be removed from the filtered list will be considered by the Technical Support Team and Designated Safeguarding Lead. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online 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 Online 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" (e.g. trainee teachers, visitors) onto the school system. Users' agreement to this policy is recorded in the Staff / Volunteer / Visitor Acceptable Use Policy
- 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 (e.g. 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.
-

16. Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Student Acceptable Use Policy and the Staff and Volunteer Acceptable Use Policy.
Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Policy. Personal email accounts are not permitted to be used for conducting school business. Any email that contains sensitive or personal information is only sent using secure and encrypted email.
Staff members and pupils are required to report spam and junk mail to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources must be deleted without being opened or attachments accessed. An annual assembly will be organised where an explanation will be given of what a phishing email and other malicious emails might look like – this assembly includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

This information will also be delivered to students through their Lifeskills lessons.

Any cyber-attacks initiated through emails are managed in line with the Data and Cyber-security Policies and Disaster Recovery Plan.

17. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.
Staff receive annual training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Staff should never look at students' personal online profile pages. Should this happen by accident, staff should report this to the DSL. If a member of staff thinks there may be a genuine reason to check a child's personal profile, they would discuss this with the DSL before making the search. This search should only be done for safeguarding purposes. Staff should not risk looking at any images that may be illegal. If this is a possibility the school would contact the police to make the search.
Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL and headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.
Pupils are taught how to use social media safely and responsibly through the online safety curriculum.
Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the Social Media Policy. The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access the school's social media accounts.
All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

18. The school website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.
The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

19. Use of devices

School-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop (when requested)
- Tablet (iPad)
- Mobile phone (key school personnel – to be agreed)

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons and for completing school work at home.

School-owned devices are used in accordance with the Device User Agreement. Pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen. All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.
ICT technicians review all school-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programs can be downloaded onto a device without authorisation from ICT technicians.
Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behaviour Policy respectively.

Personal devices

Personal devices are used in accordance with the following set of rules. Any personal electronic device that is brought into school is the responsibility of the user.
Personal devices are not permitted to be used in school.
Staff members are not permitted to use their personal devices during lesson time, other than in an emergency or for using 2FA. Staff members are not permitted to use their personal devices to take photos or videos of pupils.
Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Keeping Children Safe in Education policy.
Pupils are not permitted to use their personal devices during the school day. If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.
Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Pupils' devices can be searched, screened and confiscated in accordance with the Behaviour Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.
Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

20. Remote learning

Any remote learning implemented is delivered in line with this Policy and the Keeping Children Safe in Education Policy, along with any current and applicable legislation.
The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.
The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.
During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

21. Use of digital images (photographs and 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 e.g. 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.

22. Content Access Guidance, Breach Response Advice and Sanctions

	Staff and other adults				Students/Pupils			
	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	X				X			
Use of mobile phones in lessons		X						X
Use of mobile phones in social time	X							X
Taking photos on mobile phones	X							X
Taking photos on PC devices	X					X		
Use of personal email addresses in school or on school network				X				X
Use of school email for personal emails	X					X		
Use of chat rooms/facilities	X							X
Use of instant messaging	X					X		
Use of social networking sites				X				X
Use of blogs	X					X		

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, VS 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: **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:**	Acceptable	Acceptable for nominated	Unacceptable	Unacceptable and illegal
child sexual abuse images				x
promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation				x
adult material that potentially breaches the Obscene Publications Act in the UK				x
criminally racist material in UK				x
pornography			x	
promotion of any kind of discrimination			x	
promotion of racial or religious hatred			x	
threatening behaviour, including promotion of physical violence or mental harm			x	
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			x	
Using school systems to run a private business			x	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGFL and / or the school			x	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions			x	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)			x	
Creating or propagating computer viruses or other harmful files				x
On-line gambling		x		
On-line shopping / commerce		x		
File sharing in accordance with Penryn College's policies		x		
Use of social networking sites		x		
Use of video broadcasting e.g. YouTube		x		

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. In all cases the first point of reporting will be the DSL.

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

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

Turn off any computer / device involved immediately at the power source. Do not log off first as this may remove any evidence required later. Do not view any of the suspected content. Report the incident immediately to the DSL who will contact the Police.

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. Report the incident to the DSL who will take the appropriate action.

Sanctions for misuse

Sanctions For 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).		x	
Unauthorised use of non-educational sites during lessons	x		
Unauthorised use of mobile phone / digital camera / other handheld device (see also Mobile Phone Policy)	x		
Unauthorised use of social networking / instant messaging / personal email		x	
Unauthorised downloading or uploading of files		x	
Allowing others to access school network by sharing username and passwords		x	
Attempting to access or accessing the school network, using another student's / pupil's account		x	
Attempting to access or accessing the school network, using the account of a member of staff		x	
Corrupting or destroying the data of other users		x	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x	x
Continued infringements of the above, following previous warnings or sanctions			x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	
Using proxy sites or other means to subvert the school's filtering system		x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	
Deliberately accessing or trying to access offensive or pornographic material		x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x

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 Designated Safeguarding Lead and theincident 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

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).			x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		x	x
Unauthorised downloading or uploading of files		x	
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		x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner		x	x
Deliberate actions to breach data protection or network security rules			x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x	x
Using **personal** email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x	x
Actions which could compromise the staff member's professional standing	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x
Using proxy sites or other means to subvert the school's filtering system		x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	
Deliberately accessing or trying to access offensive or pornographic material			x
Breaching copyright or licensing regulations			x
Continued infringements of the above, following previous warnings or sanctions			x

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 Online 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.

Appendix 1

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 Online Safety and are involved in the education andguidance 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 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, Online 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 Online 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 will not use removal storage devices unless provided by ICT department.
- Unless otherwise agreed with the Head Teacher, personal mobile phones will not be used for accessing Microsoft 365 in any respect. Personal mobile phones may however be used for authentication purposes.
- I understand that the rules set out in this agreement also apply to use of school-owned mobile devices (e.g. laptops and iPads) and school systems (e.g. e-mail) out of school;
- I will change my Penryn College access password every 6 months as a minimum and to protect my own personal accounts and those of the school, my Penryn College password will not be used for any other purpose.
- 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 and the Penryn College Code of Conduct and Online Safety policies
- 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 understand that I will not allow anyone to access any school-linked device or program that I am logged into and not knowingly access any school-linked device or program that someone else is logged into;
- 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 and have checked the school parental permissions register.
- I will not use any chat or social networking sites in school and I will not befriend any current pupils, or former pupils within 5 years of them leaving the 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 unattended I will make sure I lock it to secure my accounts.

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

- If I want to use my personal handheld / external devices (PDAs/laptops) to access school systems (either cloud or server based), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. These rules comprise, but are not limited to;
- 2 Factor Authentication will be used prior to first use.

- Any PC/laptop I use accessing a school Microsoft 365 or similar will have a separate account and will not be accessible to other householders or family members.
- Removable storage devices containing information related to the school will not be used on any non-Penryn College issued device
- I will not download any school documents to my personal device – these will remain within Microsoft 365 and will be accessed remotely.
- I will not attempt to access the Virtual School on any personal, non- Penryn College device.
- I will also follow any additional rules set by the school about such use, I will ensure that any such personal 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 ICT Support Team) 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 2018 / UK GDPR. Where personal data is transferred outside the secure school network, I understand that it must be encrypted and/or password protected. This applies to any information that allows the identification of an individual, including students' work;
- 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 is 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;
- If sending a message multiple recipients who are external to the school network, such as groups of parents, I will ensure I only BCC all the recipients.

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, or 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.

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 e.g.) 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: Student Mobile Device Acceptable Use Policy

March 2023 **Date for Review:** May 2026

Introduction

Penryn College may grant a licence to use iPads / Laptops or other mobile digital devices (together referred to as "iPads / Laptops" in this policy) to 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 / Laptops and is supplementary to the college's other Acceptable Use Policies for ICT. iPads / Laptops are a privilege that carry responsibility and behavioural expectations consistent with all college rules and policies [Behaviour Policy, Acceptable Use Policy for ICT]. iPads / Laptops 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 / Laptops 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 / Laptops and compliance with this policy. This includes responsibility for the use of iPads / Laptops through internet connections at the student's home, or at a site other than the college.

Equipment

1. Each iPad / Laptop 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 / Laptop 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 / Laptop. The iPad / Laptop will be kept away from liquids, heat and protected at all times by the supplied case (in the case of iPads) which is a requirement of the Insurance cover. Laptops for home use will be transported in the supplied laptop bag.
3. The iPad / Laptop will be used for the purpose of accessing information and as a tool to enhance learning. During lessons, iPads / Laptops 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 / Laptops must be looked after, provide suitable protection to the device and remain free of writing, drawing, stickers, labels or skins, unless provided or authorised by the college. Accidental damage should be reported to ICT for repair.
5. For use outside the college, it is the responsibility of parents / carers to provide access to an appropriate internet connection. The iPad / Laptop configuration will cause all connections to be routed via the college internet filter and will log websites accessed by each device.
6. While using the device in or outside of 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 / Laptops 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 / Laptop.
8. The iPad / Laptop will, at all times, remain the property of the college. The college reserves the right to recall the iPad / Laptop or confiscate the iPad / Laptop 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 iPad mains chargers and cables into school as these are not PAT tested.

Security and Privacy

1. Passwords / pin codes must not be shared except with parents / carers and will be changed as directed by the college. Parents / carers 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 / Laptop. 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. 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 / Laptop available immediately for sampling.
5. All iPads / Laptops must have a lock code or password enabled. iPads 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. Laptops must be screen-locked if being left logged in and unattended.
6. iPads / Laptops must never be left unattended in a public place, either on college premises or elsewhere. Nor should the iPad / Laptop be left in plain sight within a vehicle. Lockers are available in college for students to store their iPads / Laptops and other valuables.
7. In the event that the iPad / Laptop is lost, damaged or stolen, this must be reported to the college immediately. If the iPad / Laptop is broken or damaged, it must be taken immediately to the IT Support team for an evaluation. If the iPad / Laptop is lost or stolen, police must be notified by parents / carers stating that Penryn College is the aggrieved party. The college reserves the right to report the incident directly should the family fail to report it. There will be a discretionary charge payable by parents / carers, the level of which is to be determined by the college, towards replacement or repair costs should the iPad / Laptop be damaged, lost or stolen as a result of recklessness or negligence. The college will also make a charge for the supply of replacement charging leads, USB plugs and iPad / Laptop cases which are lost, stolen or damaged, if deemed appropriate.

Monitoring

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

The following sections provide greater guidance on usage and restrictions.

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 / Laptop.

Use of email

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

Use of social media

1. Initially the college iPad / Laptops will not be able to access social media. In future, access to Social Media platforms will be in accordance with current school policy and will be published in the school Online Safety Policy document.
2. In general the use of email and messaging networks within lessons is permitted only where required 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 / Laptops. 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. In future, students will not be permitted to use the machines for this purpose unless their tutor and parents / carers agree that they have earned this privilege and it is in accordance with current school policy.
2. The taking of photographs and video, and other digital images, using the college's iPads / Laptops 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 / carers to take images of students is requested annually by the college. Only images that have parental / carer consent will be used by the college for the purpose of marketing or reporting.
7. The use of iPads / Laptops 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 iPad / Laptops

1. The use of iPads / Laptops outside college for personal activities is permitted, providing the student complies with this policy. All activities on the iPad / Laptop 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 / Laptops

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

Costs

When the student leaves the college, the iPad / Laptop, case and charging equipment will be returned to the college. Deliberate or reckless actions by students which result in damage, loss or theft will result in parents / carers being asked to pay a charge or, at the College's discretion, the full cost of repair or replacement. Repeated loss, damage or theft may result in the iPad / Laptop not being available to the student outside of the college or it being withdrawn altogether.

The current price list for devices, parts and accessories is published on the school website.

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 / carers. The policy will be reviewed at least annually. This policy must be read carefully by

parents / carers and students. Use of the college's iPads / Laptops 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 / Laptops) owned by the college.

Mobile Device Acceptable Use Policy Summary

The items listed below form the agreement between parent / carer, students and the college regarding the provision of Mobile Devices (hereafter iPad / Laptop) for students. More information is in the full policy, available on our website and has been e-mailed to parents.

I will report any loss, theft or damage to the iPad / Laptop to the College's ICT Support team or my teacher 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 college will make a charge to parents / carers in the case of loss, theft or damage to the iPad / Laptop *resulting from failure to take proper care of it*. A charge will also be raised for repeated damage caused due to lack of care of the device. The college will also make a charge for the supply of replacement charging leads, USB plugs and iPad / Laptop cases which are lost, stolen or damaged in any way due to repeated negligence or malicious intent. A list of current charges is attached to this document, is posted on the school website and is also available on request.

In signing this summary sheet students are indicating agreement to the above and to the following, parents are signing to indicate their understanding of, and support for the student responsibilities:

- I will not use inappropriate, abusive or discourteous language when sending any electronic communications (e.g. email) or encourage others to use such language.
- I will not use my iPad / Laptop 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.
- I will use my iPad / Laptop in lessons in the way in which I am asked, and follow the instructions given by the teacher.
- I understand that the iPad / Laptop is provided for learning. Any work, files, apps, games, photos or videos on the iPad
- / Laptop are stored at the college's discretion and I will remove them if asked to do so.
- 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.
- 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.
- I will never leave the iPad / Laptop in an unsecured or unlocked place.
- I will inform the IT Support 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 / Laptop by another student.
- I will charge the iPad each evening at home and bring it into college every day.
- I will ensure that the iPad is always suitably covered by the provided case with screen protection or the laptop is protected by the supplied case when being transported.
- I will not take any action that has the potential to damage the iPad / Laptop or the iPad / Laptop belonging to another student or member of staff.
- I will return the iPad / Laptop, case and charging equipment to the college on request. I understand that the iPad / Laptop, case and charging equipment remain the property of the college.
- I understand that the iPad / Laptop is provided for the purpose of learning and education and I will use the device for this purpose. Apps installed other than for this purpose will be removed on request by the college.
- I will protect the iPad / Laptop with a pin code/ password. I will share this password only with my parents / carers and no-one else. I will share my code with them so they can access my iPad / Laptop when they want to. I will not use or attempt touse the password of another student.
- I understand that the use of the iPad / Laptop will be monitored by the college and that there is no right to privacy when using the iPad / Laptop. I understand that any activity carried out on the iPad / Laptop may be monitored by the college.
- 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 / Laptop etc. The college will involve the police or other agencies if appropriate.

Students name (Please print)**:** **Students signature:** **TG**:

[ ] I acknowledge that I have read and understood the full version of this Acceptable Use Policy

OR

[ ] I am unable to access the link provided and require a paper copy (I understand until this is signed and returned my child will not be able to receive their iPad)

Name of parent/carer (Please print):

Date: Signature:

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 Online 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 Online Safety individual support programme, it is important that we ensure our studentsare 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	

Nature of Risk:	Level of risk (1-5)*
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		