PENINSULA LEARNING TRUST

Penrice Academy

ONLINE SAFETY POLICY

Adopted by the Governing Body on July 2017
Review date: December 2018

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

Roles and Responsibilities
The following section outlines the roles and responsibilities for the online safety of individuals and groups within the Academy:

Governors:
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

Principal and Leadership Team:
- The Principal is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinators.
- The Principal and Leadership Team are responsible for ensuring that the Online Safety Coordinators and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinators.
- The Principal and Online Safety coordinators are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Online Safety Coordinators are: Gary Henderson and Jane Nicholas.
Online Safety Co-ordinators:
- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the Academy online safety policies and documents.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff

- liaise with the Local Authority
- liaise with Academy ICT technical staff
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- attend relevant meeting / committee of Governors
- report regularly to Leadership Team

Network Manager / Technical staff:
The Network Manager is responsible for ensuring:
- that the Academy's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the Academy meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the Academy's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- that he / she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinators for investigation
- that monitoring software and systems are implemented and updated as agreed in the Academy policies

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

Designated Safeguarding Lead
should be trained in online safety issues and be 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
- cyber-bullying

Students
- are responsible for using the Academy ICT systems in accordance with the Student Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand Academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Academy policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of the Academy and realise that the Academy's Online Safety Policy covers their actions out of the Academy, if related to their membership of the Academy

Parents / Carers
Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The Academy will therefore take every opportunity to help parents understand these issues through newsletters, letters, website / VLE and information about national and local online safety campaigns and literature. Parents and carers will be responsible for:
- endorsing (by signature) the Student Acceptable Use Policy
- accessing the Academy website / VLE in accordance with the relevant Academy Acceptable Use Policy.

Online safety education will be provided in the following ways:
- A planned online safety programme is provided as part of ICT and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in and outside the Academy
- Key online safety messages are reinforced as part of a planned programme of assemblies
- Students are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students are 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 the Academy
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all ICT rooms and displayed on log-on screens
- Staff will act as good role models in their use of ICT, the internet and mobile devices

The Academy will therefore seek to provide information and awareness to parents and carers through:
- Letters, newsletters, web site, VLE
- Parents evenings

Curriculum
Online Safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

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

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy 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 Academy 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 students will be selected carefully and will comply with good practice guidance on the use of such images.
- Consent from parents/ carers will be sought at the start of each year regarding the use of images.
- Student's work can only be published with the permission of the student and parents or carers.

Data Protection
Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with Academy policy (below) once it has been transferred or its use is complete

Communications

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

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the Academy	X				X			
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones or other camera devices		X*					X*	
Use of hand held devices eg PDAs, PSPs		X*					X*	
Use of personal email addresses in the Academy, or on the Academy network	X							X
Use of Academy 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	

- Use of mobile phones in social times by staff should be discreet and not visible to students.
- There are occasions when the curriculum requires students to take photos. This must be with the express permission of staff and in accordance with Academy polices.

Responding to incidents of misuse by students

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights*	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).					X	X	X		X
Unauthorised use of non-educational sites during lessons	X				X	X	X		
Unauthorised use of mobile phone / digital camera / other handheld device	X*								
Unauthorised use of social networking / instant messaging / personal email	X*								
Unauthorised downloading or uploading of files	X				X	X	X		X
Allowing others to access school network by sharing username and passwords	X	X			X	X	X		X
Attempting to access or accessing the Academy network, using another student's account	X	X			X	X	X		X
Attempting to access or accessing the Academy network, using the account of		X	X		X	X	X		X

a member of staff									
Corrupting or destroying the data of other users		X			X	X	X		X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X (H0Y)	X		X	X	X		X
Continued infringements of the above, following previous warnings or sanctions		X	X				X		X
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy		X	X	X			X		X
Using proxy sites or other means to subvert the Academy's filtering system		X			X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X	X		X	X	X	X

Responding to incidents of misuse by staff

Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Principal	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).				X		X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X				X		X
Unauthorised downloading or uploading of files	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the Academy network, using another person's account	X				X		X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X		X	X		X
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out	X	X	X			X	X

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