PENINSULA
LEARNING TRUST

Lostwithiel Primary School

Online Safety POLICY

Adopted by the Governing Body on July 2016
Review date: July 2017

Scope of the Policy
This policy applies to all members of the Academy (including staff, pupils, 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 e-safety of individuals and groups within the Academy:

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

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

E-Safety Coordinator:
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the Academy e-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with Academy ICT technical staff

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- attends relevant meeting / committee of Governors
- reports 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 e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-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 e-safety technical information in order to effectively carry out their e-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 E-Safety Co-ordinator 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 e-safety matters and of the current Academy e-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 E-Safety Co-ordinator for investigation
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and are carried out using official Academy systems
- e-safety issues are embedded in all aspects of the curriculum and other Academy activities
- pupils understand and follow the Academy e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended Academy activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current Academy policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead
should be trained in e-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

Pupils

- 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 e-safety practice when using digital technologies out of the Academy and realise that the Academy's E-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 e-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.

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

- A planned e-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 e-safety messages are reinforced as part of a planned programme of assemblies
- Pupils 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
- Pupils 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
- Pupils 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
- Parents evenings

Curriculum

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

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils 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, pupils 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.
- Pupils 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
- Pupils 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 pupils 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Pupils 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.
- 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

Mobile Phones:

Staff: Staff may bring their own mobile phone onto the school site. However, at no point during the school day (8:30-3:15) should mobile phones be visible. Staff are requested to leave phones off or on silent locked safely in a drawer or their bag or left in the staff house.

During residential/ trips staff may take their mobile phone to contact school.

Staff should not take images or photos on personal devices. School ipads and cameras should be used.

Pupils may need to bring a mobile phone into school if they walk home alone. These should be given to their class teacher in the morning where it will be locked safely away until the end of the school day.