PENINSULA LEARNING TRUST

# Lostwithiel School

## ONLINE SAFETY POLICY

Adopted by the Governing Body on November 2017
Review date: November 2018

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

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

**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.

**Headteacher and Leadership Team**:
- The Headteacher 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 ICT lead.
- The Headteacher and Leadership Team are responsible for ensuring that the ICT lead and other relevant staff receives suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and ICT lead 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 headteacher and ICT lead will:
- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the School 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 PLT 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

**PLT Network Manager / Technical staff**:
The Network Manager is responsible for ensuring:

- that the School's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the School 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 School's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- 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 / 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 School 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 School online safety policy and practices
- they have read and understood the School Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the designated safeguarding lead for investigation
- online safety issues are embedded in all aspects of the curriculum and other School activities
- pupils understand and follow the School online safety and acceptable use policy
- they monitor ICT activity in lessons, extra-curricular and extended School 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 School policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

**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

**Pupils**

- 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 School policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand School policies on the taking / use of images and on cyber-bullying.

- should understand the importance of adopting good online safety practice when using digital technologies out of the School and realise that the School's Online Safety Policy covers their actions out of the School, if related to their membership of the School

**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 School will therefore take every opportunity to help parents understand these issues through newsletters, letters, website and information about national and local online safety campaigns and literature.

**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 School
- Key online safety messages are reinforced as part of a planned programme of assemblies
- Pupils are taught in all lessons to be aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the School
- Rules for use of ICT systems / internet will be posted in all classrooms
- Staff will act as good role models in their use of ICT, the internet and mobile devices

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

- Letters, newsletters, web site,
- 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 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 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School 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 this policy 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 school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

- Use of mobile phones in social times by staff should be discreet and not visible to pupils. This should only be in the school office, staff or PPA room in line with mobile phone guidance in staff handbook.
- There are occasions when the curriculum requires pupils to take photos. This must be with the express permission of staff and in accordance with School polices.