**Ashton on Mersey SCITT E-Safety Policy**

**Author: S Buckley Date written/amended: 23rd May 2017**

**Date of next review: 23rd May 2018**

**Introduction**

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The e-safety policy should operate in conjunction with other policies including those for trainee Behaviour, Bullying, Curriculum, The Dean Trust’s Acceptable Usage Policy, Data Protection and Security.

**E-safety policy**

**Why Internet use is important**

* The Internet is an essential element in 21st century life for education, business and social interaction. The SCITT has a duty to provide trainees with quality Internet access as part of their learning experience
* Internet use is a part of the statutory curriculum and a necessary tool for trainees.

**Internet use will enhance learning**

* Trainees will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
* Internet access will be planned to enrich and extend learning activities
* SCITT facilitators will guide trainees in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

**E-Safety on Placement**

* If trainees discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT Coordinator
* If trainees are taking pupils out of school they must NEVER pass on their personal mobile numbers to pupils or their parents. If they have to pass on a mobile number, which is good advice for trips, it must be the school mobile number, never a personal one. Never telephone parents from a personal or home phone number
* With regards to email, trainees can contact parents via a work email address, NEVER a personal one and it is ill advised to email pupils directly from either a work one or a personal one
* Social networking sites and newsgroups will be blocked unless a specific use is approved.
* The Headteacher will ensure that the school e-Safety Policy is implemented and compliance with the policy monitored.

**Internet use - Possible teaching and learning activities**

|  |  |  |
| --- | --- | --- |
| **Activities** | **Key e-safety issues** | **Relevant websites** |
| Creating web directories to provide easy access to suitable websites. | Pupils should be supervised.  Pupils should be directed to specific, approved on-line materials. |  |
| Using search engines to access information from a range of websites. | Pupils should be supervised.  Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. | Web quests e.g.  Ask Jeeves for kids  Yahooligans  CBBC Search  Kidsclick  Picsearch  safesearch  **NOT Google images** |
| Exchanging information with other pupils and asking questions of experts via e-mail. | Pupils should only use approved e-mail accounts.  Pupils should never give out personal information.  Consider using systems that provide online moderation e.g. SuperClubs. | GridClub  School Net Global  Kids Safe Mail  E-mail a children’s author  E-mail Museums and Galleries |
| Publishing pupils’ work on school and other websites. | Pupil and parental consent should be sought prior to publication.  Pupils’ full names and other personal information should be omitted. | School website  Learn Premium  Espresso |
| Publishing images including  photographs of pupils. | Parental consent for publication of photographs should be sought.  Photographs should not enable individual pupils to be identified.  File names should not refer to the pupil by name. | School website |
| Communicating ideas within chat rooms or online forums. | Only chat rooms dedicated to educational use and that are moderated should be used.  Access to other social networking sites should be blocked.  Pupils should never give out personal information. | GridClub |
| Audio and video conferencing to gather information and share pupils’ work. | Pupils should be supervised.  Only sites that are secure and need to be accessed using an e-mail address or protected password should be used. | City Learning Centres |