Keeping Children Safe Online Policy

Introduction

At Attenborough School we take Internet Safety very seriously and see it as our duty to keep our pupils safe whilst using technology not only in school but also at home. This also includes our responsibility to keep our children safe from radicalisation and extremism (Prevent Duty).

This document has been written in collaboration with DCYP, MoD Schools HQ and adopts best practice E-Safety guidance from a number of leading U.K. Local Authorities. It has also followed guidance from the Revised Prevent Duty document (HM Government, July 2015).

The policy covers 3 main areas; children's safety, staff's responsibilities and support for parents.

Network Safety

The school Network is managed by DCYP MoD Schools IT infrastructure team who work closely with British Army HQ IT & MoDNET to ensure a very secure school network. School network firewalls protect our children in school and filter out or block undesirable online content.

Regular face-to-face or 'TEAM' meetings takes place between the IT team, computing lead and a senior leader. During these meetings any issues with the Network and E-Safety issues are dealt with.

Safety and Responsibilities for Staff

All staff are required to read and sign an Acceptable User Policy (AUP) which clearly states the responsibilities of staff using technology in the work place. This will be signed when they commence their employment at Attenborough School and will be re-enforced each year during the staff's E-Safety Safeguarding Session.

All staff will attend both training on E-Safety and Prevent (dealing with radicalisation & extremism).

The AUP list the responsibilities of all staff and covers the use of digital technologies in school: i.e. **E-mail, Internet, Intranet and network resources,** Learning Platform, software, **equipment and systems and complements the** General Teaching Council's Code of Practice for Registered Teachers**.**

Keeping Children Safe Online Policy

All staff will agree to the following:

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and School Governing Committee.
- I will not reveal my password(s) to anyone. I will not log on for another person.
- I will not allow unauthorised individuals to access E-Mail / Internet / MODNET/ or other online accounts.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I understand that there is a difference between my professional and private roles. I will not engage in any online activity that may compromise my professional responsibilities, this refers to social network sites such as Facebook. (Refer to Social Network Policy)
- I will only use the approved, secure E-Mail system(s) for any school business.
- I will only use the approved school E-Mail, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- At any time, I will not use school equipment to browse, download or send material that could be considered offensive or inappropriate to colleagues or pupils.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact (Chris McCarthy (DHT) or Andy Chapman (HT)).
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will report any concerns I have about a child accessing inappropriate material on the Internet, including pornography, extremism, radicalisation and violence.
- I will not connect a personal computer, laptop or other device to the network / Internet that does not have authorisation to do so.
- I will not use personally owned digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer, laptop or IPad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school if a reasonable amount of personal use outside of school hours becomes "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information

management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will embed the school’s E-Safety curriculum into my teaching.
- I understand that all Internet usage / and network usage is monitored and that monitoring data could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

E-Safety and Prevent training will be provided to all members of staff at least once a year and it is each person’s responsibility to attend this session. These sessions will be arranged by the Computing Lead and/or Deputy Headteacher.

It is very important that staff make sure that pupils they are responsible for are using the Internet safely. High risk students will be highlighted by class teachers and appropriate staff will be made aware of these students.

Safety and Responsibility for Pupils

Although some of our pupils are unable to access the Internet we have a good percentage of pupils who are able to use the Internet independently and therefore are at risk from either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites.

No child is able to access the Internet in school without their parents giving permission to do so. This consent form is filled in and submitted to the school office during initial admission. All children are supervised in school whilst using the Internet and all are made aware that all their activity within school is monitored.

All pupils will receive E-Safety training at the beginning of each term, either as part of their ICT session or PHSE session. (All E-Safety materials including lessons plans, PowerPoints and videos are stored on the school network). All pupils will be taught how to use all technologies in a responsible and safe way. This will be part of the Computing Curriculum.

No child may appear on the Web Site without their parent/carers consent, the consent form is completed at enrolment.

Keeping Children Safe Online Policy

Support for Parents

As a school we believe it is our duty to support parent and carers in keeping their child safe while using technology within the home environment. Computers and other devices in the home are more open and don't have the security features which we have in school, which does make the child more vulnerable in this environment.

The school web site will have information regarding E-Safety for parents / carers and young people and this information will be updated on a regular basis.