

Astmoor Primary School

**E-SAFETY POLICY**

|  |  |
| --- | --- |
| Recommended by: | Mrs Aldridge |
| Approved by: | Curriculum Committee |
| Approval Date: |  |
| Review Date: |  |

**Introduction**

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

 • content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

 • contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

 • conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

* Websites
* Virtual Learning Platforms
* Email and Instant Messaging
* Chat Rooms and Social Networking
* Forums, Wikis and Blogs
* Podcasting
* Video Broadcasting
* Music Downloading
* Gaming
* Mobile/ Smart phones with text, video and/ or web functionality
* Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

We understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises utilising the school’s network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

**Roles and Responsibilities**

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named e-Safety co-ordinator in our school is **Mrs Aldridge** who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Halton LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head or e-Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school’s acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

**E Safety skills development for staff**

* Our staff receive regular information and training on e- Safety issues in the form of regular staff training.
* New staff receive information on the school’s acceptable use policy as part of their induction.
* All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e Safety and knowwhat to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
* All staff are encouraged to incorporate e Safety activities and awareness within their curriculum areas.

**Managing the school E Safety messages**

* We endeavour to embed e Safety messages across the curriculum whenever the internet and/or related technologies are used.
* The e-safety policy will be introduced to the pupils at the start of each school year.
* E-safety posters will be prominently displayed.

**The Prevent Duty**

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.   
  
More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school’s ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

* Internet searches for terms related to extremism
* Visits to extremist websites
* Use of social media to read or post extremist material
* Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose.

**E Safety in the Curriculum**

* Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e Safety curriculum.
* Pupils are taught about copyright and respecting other people’s information, images, etc. through discussion, modelling and activities.
* Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/CEOP report abuse button.

**Password Security**

* All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school’s e-safety Policy.
* Users are provided with an individual network, email and Learning Platform log-in username.
* Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
* If you think your password may have been compromised or someone else has become aware of your password report this to the Head teacher
* Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS MIS systemand/or Virtual Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
* Due consideration should be given when logging into the Virtual Learning Platform to the browser/cache options (shared or private computer)
* In our school, all ICT password policies are the responsibility of the Head teacher and all staff and pupils are expected to comply with the policies at all times.

**Data Security**

The accessing of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008).   
Staff are aware of their responsibility when accessing school data. They must not;

* allow others to view the data
* edit the data unless specifically requested to do so by the Head teacher.

**Managing the Internet**

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Halton Internet Web Filtering Systems** is logged and the logs are randomly monitored. Whenever any inappropriate use is detected it will be followed up by Halton Borough Council through its e Safety responsibilities.

* Pupils will have supervised access to Internet resources (where reasonable) through the school’s fixed and mobile internet technology.
* Staff will preview any recommended sites before use.
* Raw image searches are discouraged when working with pupils.
* If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
* All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
* All users must observe copyright of materials from electronic resources.

**INFRASTRUCTURE**

Halton Local Authority has a monitoring solution where web-based activity is monitored and recorded.

* School internet access is controlled through the LA’s web filtering service.
* The school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
* Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
* The school does not allow pupils access to internet logs.
* The school uses management control tools for controlling and monitoring workstations.
* If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
* It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
* Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head teacher.

**Managing other Web 2 technologies**

Web 2/Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

* At present, the school endeavours to deny access to social networking sites to pupils within school. It is also noted that the age of the children would suggest that they are too young to sign up to social networking sites but may have access to them. Therefore all the advice and teaching is given in context of being SMART on line.
* All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
* Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
* Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
* Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
* Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
* Our pupils are asked to report any incidents of bullying to the school.
* Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Head teacher.

**Mobile technologies**

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

**Personal Mobile devices (including phones)**

* The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
* On rare occasions, when an older pupil (year 5/6) brings a personal device or mobile phone to school, they are stored in the school office during the day.
* The school is not responsible for the loss, damage or theft of any personal mobile device.
* The sending of inappropriate text messages or emails between any member of the school community is not allowed.
* Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
* Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
* Staff should not contact pupils outside normal school hours.

**School provided Mobile devices (including phones)**

* The sending of inappropriate text messages between any member of the school community is not allowed.
* Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
* Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
* Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

**Managing email**

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good ‘netiquette’.

* Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
* The school requires a standard disclaimer to be attached to all email correspondence, stating that, ‘the views expressed are not necessarily those of the school or the LA’. The responsibility for adding this disclaimer lies with the account holder.
* E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
* Staff sending emails to external organisations, parents or pupils are advised to cc. the Head teacher, line manager or designated account.
* Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
* Children use a class/group email address.
* The forwarding of chain letters this includes jokes and funny statements are not permitted in school.
* All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
* Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
* Staff must inform (the e-Safety co-ordinator/ line manager) if they receive an offensive e-mail.
* Pupils are introduced to email as part of the ICT Scheme of Work.

**Safe Use of Images - Taking of Images and Film**

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

* With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
* Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school’s network and deleted from the staff device.
* Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school’s network and deleted from the pupils device.

**Publishing pupil’s images and work**

On a child’s entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

* on the school web site
* on the school’s Learning Platform
* in the school prospectus and other printed publications that the school may produce for promotional purposes
* recorded/ transmitted on a video or webcam
* in display material that may be used in the school’s communal areas
* in display material that may be used in external areas, ie exhibition promoting the school
* general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child’s circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils’ names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils’ full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

**Storage of Images**

* Images/ films of children are stored on the school’s network
* Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head teacher
* Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
* **Mrs Aldridge** has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

**Webcams and CCTV**

* We do not use publicly accessible webcams in school.
* Webcams in school will only ever be used for specific learning purposes, i.e. monitoring hens’ eggs and never using images of children or adults.
* Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ‘ inappropriate materials’ section of this document)
  + Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

**Video Conferencing**

* Permission is sought from parents and carers if their children are involved in video conferences
* Permission is sought from parents and carers if their children are involved in video conferenceswith end-points outside of the school.
* All pupils are supervised by a member of staff when video conferencing
* All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
* The school will keep a record of video conferences, including date, time and participants.
* Approval from the Head teacher is sought prior to all video conferences within school.
* The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
* No part of any video conference is recorded in any medium without the written consent of those taking part.

**Misuse and Infringements**

**Complaints**

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Head teacher. Incidents should be logged on.

**Inappropriate material**

* All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator.
* Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
* Users are made aware of sanctions relating to the misuse or misconduct by formal interview and follow up letter from the Head teacher.

**Pupils with additional needs**

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools’ e-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children.

**Parental Involvement**

.

* Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
* Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website).
* The school disseminates information to parents relating to e-Safety where appropriate in the form of;
* Information and celebration evenings
* Posters
* Website/ Learning Platform postings
* Newsletter items
* Learning platform training

**Writing and Reviewing this Policy**

**Review Procedure**

There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.