

## Arden Primary School. E-Safety Policy.

This E-Safety Policy is built on the following five core principles:

- Guided educational use
- Risk assessment
- Regulation
- Responsibility
- Appropriate strategies

Arden Primary School believes in the educational benefits of curriculum Internet use. Its purpose in school is to raise educational standards; to promote pupil achievement, to support the professional work of staff and to enhance the school's management systems. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Teachers need the internet to plan, to integrate the use of communications technology such as web-based resources in delivering the curriculum and make full use of e-mail to communicate with support services, professional associations and colleagues at all levels to ensure effective management. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill. However, the school management recognises that there are risks and dangers as well as benefits associated with internet use. This E-Safety Policy is to ensure appropriate, effective and safe use by both pupils and staff.

No child will use the internet without a teacher or responsible adult giving permission **and being present**. This excludes internet use by children when with their dinner ladies during wet lunchtimes. Internet access can be achieved very quickly by children, who may follow links quite innocently into areas unsuitable for them, or be used by NET skilled children who can easily disguise the fact that they are both doing their set task and are also using the internet for their personal interests! Staff using computers with children are advised to be aware of what the children are doing and therefore what is being explored because of the potential risks.

Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Any adult taking responsibility for children using the internet must do so in the full knowledge of information contained in this document. At no time must children be left unattended while on the internet or using any computer capable of accessing the internet.

Staff using the internet within their classrooms to display web sites, (especially on interactive whiteboards) are advised to assess the sites suitability, along with any links from the site to make sure the material is appropriate. This increasingly applies when using search engines, such as Google, especially image searches which may include inappropriate pictures that are not filtered out by our protection software, in the results. Staff must check all search results that they are going to use with children prior to the lesson. Making spontaneous searches that do not allow staff to check the results should only be done on recognised highly regarded sites such as the bbc.co.uk . Staff should recognise that miss-spelling words in searches can lead to inappropriate material being viewed by children. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Staff and children are made aware that although Internet use at school is subject to an anti virus and an inappropriate material filter system, the school cannot guarantee this will be effective 100% of the time. Filtering, anti-virus and firewall protection are all provided by the Birmingham Grid For Learning. (Bgfl) Wherever possible settings for filtering will be at the strictest levels i.e Google – Preferences – Strict filtering.

This policy along with the schools overall code of conduct aims to add other safeguards to online internet activity.

If while using the internet with children something unacceptable happens, the adult will inform the SMT or Network Manager/e-safety coordinator (usually ICT coordinator) who will contact the BGfL and inform the children's parents. The URL (Uniform Resource Locator (web address)) and content must be reported to BCC using the e-mail [filtering@bgfl.org](mailto:filtering@bgfl.org). If necessary, the incident can be discussed with all staff to inform them how vigilant they need to be and how to respond to similar incidents. Once the site is reported to the Bgfl they can block the site and provide city wide protection.

Children will be taught to be "NETSMART" with responsible attitudes. This will be achieved with staff and children kept aware of the potential dangers associated with the internet, although they will be protected as far as possible in school. We encourage children to inform staff if they see anything they do not feel comfortable with. Children at Arden will be taught basic conventions and navigation techniques before going on the internet. Once they begin using the internet in school, they are directed to specific sites, either with direct links or specific URLs to type into the address space. Again staff must be aware that children can very quickly be directed out of the given website. Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. Teachers need to choose a topic with care, select the search engine and then discuss with pupils sensible search words, which again should be tested prior to the lesson. Searches to be carried out by children are carefully vetted, with the search criteria being specified where necessary, to ensure safety and suitability. Results of searches are also discussed and evaluated to enable them to judge the relevance and quality of the information to make children aware that not all information on the internet is useful and true. The way search engines and online information sites gather their information and results will be part of a Childs e-safety education. This will also include respect for copyright and intellectual property rights, and that the use of published materials by staff and by pupils complies with copyright law.

Ideally inappropriate material will not be visible to pupils using the Web but this is not easy to achieve and cannot be guaranteed, despite all attempts at filtering

Key stage 2 Pupils will be reminded of the rules and risks at the beginning of any lesson using the Internet. The habit of informing parents before they use the internet needs to be constantly reinforced . Key stage 1 pupils will always be reminded to only use the internet at home with their parents.

During the first ICT lessons a year 6 child attends, they research, discuss and present information about safe internet use. This takes place over three or four lessons and prepares them both for the work they do over the internet in year 6 and teaches them to be aware and become responsible users of the internet either at school or at home. They are made aware of the meaning and importance of being NETSMART. Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the URL to the teacher for inclusion in the list of blocked sites.

Children are given opportunities to send emails in carefully monitored lessons. They only use Whole-class e-mail accounts on the school system, or ones set up for a specific purpose. They are reminded to be NETSMART and not reveal details of themselves or others in e-mail or other forms of electronic communication, such as their address, telephone number, or arrange to meet anyone.

Access for children in school to external personal e-mail accounts is generally not allowed and the forwarding of chain letters is not permitted.

E-mail sent to an external organisation should be written carefully and authorised by a teacher before sending, in the same way as a letter written on school headed paper. Attachments are sent as part of year 6s ICT curriculum, again to carefully chosen recipients who are made aware beforehand of the intended emails from our children.

During Year 6s lunchtime computer time, access to the internet is closely monitored and subject to rules and sanctions, which all year 6 children and staff are made aware of. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. They have a folder with specific links in to guide them to appropriate sites. Information they want to copy and print has to be seen by one of the teacher / assistants monitoring the activity. They should not print directly from the website but copy and paste relevant information and present it in a word document. The children should add their own details and be set an appropriate task where applicable, to extend their search before being allowed to print.

Some Year 6 children assist staff by looking after printers and by logging on in preparation for younger groups to use large ICT suites at lunchtimes and before school. These children are not always supervised, so staff organising these children are advised to keep an interest in what the children are doing and regularly discuss the job and monitor their activities at these times.

No data, Music or video files can be downloaded by children without permission. Games involving violence, which or are not suitable for children are banned if not already blocked.

Children who do not follow these rules and do not use the internet responsibly are subject to sanctions such as a temporary or permanent ban from their lunchtime access, with any form of internet abuse being entered in the school behaviour book.

Among the sites that are currently off limits to children are unmonitored chat rooms, youtube.com or myspace.com(blocked). (unless permission is given by the teacher in consultation with a senior manager or e-safety coordinator)

There are carefully monitored chat rooms that the school could subscribe to if this was thought appropriate.

Children using their own home email accounts or accessing other children's data without permission also breach the e-safety policy.

The school website gives information that will be of interest to other schools and parents. The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published. Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified or give individual details.

Staff must understand that the rules for any Birmingham City Council employee on Internet misuse are quite specific. Instances of misuse resulting in dismissal have occurred. If staff have doubts as to the legitimacy of any aspect of their Internet use in school, they must arrange to discuss them with their line manager or e-safety coordinator, to avoid any possible misunderstanding.

All staff are governed by the terms of the 'Responsible Internet Use document' in school.

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained. Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures will in turn be supervised by senior management. Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required. Loading non-approved software could cause major problems and must only be undertaken with the consent and by the ICT coordinator or Network Manager. Good password practice is required including logout after use which will prevent pupils or other staff accessing your files or email account. If you need to change your password please ask the ICT coordinator.

Use of portable media such as memory sticks and CD-ROMs will be monitored. Portable media is provided by Arden School. Staff and pupils own media may be brought into school with permission, but will need to be virus checked before use on the network. Staff using their own phone, camera and or USB Flash Memory Stick to take and store pictures needs to be checked / confirmed with another teacher to protect both the children and member of staff concerned.

Unapproved system utilities and executable files will not be allowed in staff / pupils' work areas or attached to e-mail.

All Files held on the school's network will be regularly checked.

Staff may not use the internet for personal use during lesson times. If they use it during their own time, they do so subject to the guidelines of Birmingham's Acceptable Use Policy, issued to all members of staff. (Staff will be required to sign an internet use agreement to say they have read and understood it.)

All of the above rules also apply to students based in the school on work experience. They must be supervised if they wish to use the internet by the class teacher they are based with or sent to the ICT coordinator to agree a time when they can use a computer in the ICT suite.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the speed of change, international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BCC can accept liability for the material accessed, or any consequences of internet access. Methods to identify, assess and minimise risks will be reviewed regularly. Responsibility for handling incidents will be delegated to a senior member of staff. Any complaint about staff misuse must be referred to the head teacher.

The head teacher will ensure that the E-Safety policy is implemented and compliance with the policy monitored.

New Parents sign a general Permission Letter which along with other important agreements, gives the school permission for their child to use the Internet. Advice is also available for them at parents evenings on children using the internet at home. This will include demonstrations, practical sessions and suggestions for safe Internet use at home. The school ICT systems will be reviewed regularly with regard to security, efficiency and appropriateness. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones will not

be used during lessons or formal school time. The sending of abusive or inappropriate text messages or emails is forbidden.

Our Internet draft Policy is based on the Internet Policy document produced by Kent County Council using the Becta guidance and acknowledged by Birmingham Grid for Learning in their internet use guidance document.

Martin Jones ICT Coordinator.

The Becta e-safety document states

The overall responsibility for internet safety need not sit with the ICT coordinator or network manager but they should ensure that technologies are in place to ensure as far as possible technological solutions to support classroom practice. Ultimately the head teacher in conjunction with the governing body is responsible for internet safety.

NETSMART. Always be polite:-)

Never give your full name, passwords, phone numbers or addresses on the net.

E-mails or postings that are nasty or rude... simple delete them.

Tell your parent or carer if you see bad language or rude pictures on the internet

Someone who makes you an offer that is too good to be true, is probably lying.

Meeting anyone from the internet, you or your parents don't know is asking for trouble.

A chat room can make you feel uncomfortable or worried. If it does, get out.

Respect yourself and respect the Internet. It will as good as the people who use it.