Asterdale Primary School

E-Safety Policy

Approved by the Governing Body	:	April 2017
Next Review Due	:	April 2020

Signed: _____

The e-Safety Policy is part of the Computing Policy and School Improvement Plan and relates to other policies including those for Computing, Anti-bullying and for Child Protection.

Our e-Safety Policy has been written by the Computing Co-ordinator and the Child Protection Officer. It has been agreed by the senior management and approved by governors.

Background

Many of our pupils interact with new technologies such as mobile phones, tablets, laptops and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in a vulnerable position.

It is not possible to "police" or prohibit such use of technology which clearly has a valuable place in the everyday lives of all children and adults. We aim to educate the children to become increasingly independent and adopt safe ways of using ICT and social media. We are aware that there is a risk which is ever changing and we will support all children through encouraging them to seek the help of trusted adults should they be a victim of cyberbullying or if they feel uncomfortable with the material they encounter whilst using modern technology. We develop a culture where we foster and encourage children to feel safe in speaking freely about what they access electronically at school and home rather than to restrict and drive "underground" any potential areas of harm.

Teaching and learning

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote children's achievement, to support the professional work of staff and to enhance the school's management functions.
- The Internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide children with quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Children use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use to enhance learning

- The school Internet access will be designed expressly for children's use and will include filtering appropriate to the age of pupils. Filtering is provided though Smoothwall system.
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Evaluation of Internet content

The school will ensure that the copying and subsequent use of Internet derived materials by staff and children comply with copyright law.

- Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

Local Area Network security issues:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations are secured against user mistakes and deliberate misuse.
- The server operating system is secured and kept up to date.
- Virus protection and Firewall services for the whole network is installed and updated regularly by Link ICT.

Wide Area Network (WAN) security issues:

- Personal data will only be sent over the Internet by secured school email addresses.
- Personal on portable media will be encrypted or otherwise secured.
- Portable media may not be used by pupils without specific permission followed by a virus check. Staff may use portable media. They must be encrypted.
- Files held on the school's network will be regularly checked.
- The Computing co-ordinator Link ICT will review system capacity regularly.

Management of e-mail

Members of staff are provided with e-mail accounts. Staff e-mail addresses take the form firstinitial.surname@asterdale.derby.sch.uk. Wider access can be arranged for e-mail use for specific educational projects.

Management of published content

The school has a website. The contact details on the website are the school address, admin e-mail and telephone number. Staff or pupils' personal information is not published.

Publication of pupil's images or work

- Staff will ensure that only digital cameras provided by the school will be used to photograph pupils. Staff should not use personal mobile phones to take photographs of children, except with the specific approval of the headteacher.
- Staff will ensure that all photographs of pupils are deleted from the school digital cameras as soon as practically possible once transferred.
- Staff will ensure that no photograph or image of pupils will be transferred to personal or home computer systems this also includes personal USB devices.
- The school operates an 'opt out' policy for photograph permissions. Pupil's photographs may be published on the school website, unless parents have opted out upon admission to school.
- Pupils' full names will not be used anywhere on the school web site or other unsecured on-line space.
- Work can only be published with the permission of the pupil and parents/carers.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic hardware upon admission to school.

Management of social networking and personal publishing

- The school will block access to social networking sites.
- Pupils will be given opportunities to use the social networking tools available through the 'Switched On Computing' scheme of work to enable them to experience social networking in a secure environment.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind, which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph, which could identify the student or his/her location e.g. house number, street name or school.
- Staff should not accept minors as 'friends' on social networking sites.

- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.
- Pupils are advised not to publish specific and detailed private thoughts.
- Pupils are advised not to engage in voice chat with anyone whom they do not know personally.
- The school is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Management of filtering

Internet filtering is provided by Smoothwall.

If staff or pupils discover unsuitable sites, the URL must be reported to Smoothwall via email. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

How can emerging technologies be managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Pupil are not allowed to bring mobile phones to school, unless permission is granted by designated school staff eg class teacher or headteacher. On such occasions, mobile phones should be handed in to the class teacher. Staff have access to a school phone and messaging service where contact with parents is required.

How should personal data be protected?

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school has a Data Protection Policy in place.

Risk assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material.
- However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor DCC can accept liability for the material accessed, or any consequences resulting from Internet use.

- The school will review Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

E-safety complaints Concerns

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure. A copy of which is on the website.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the Derby Safeguarding Children's Board (DSCB) to establish procedures for handling potentially illegal issues.
- Discussions with Police will take place immediately if the school identify a risk which is beyond the "school's capacity" to support / deal with.
- School will seek support from CEOP should it be felt that information regarding online activities should be shared.

Sanctions within the school discipline policy include:

- Interview/counselling by senior member of staff.
- Informing parents or carers.
- Removal of Internet or computer access for a period.

Communicating the Policy

Introducing the policy to pupils.

- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety module is included in every unit of the 'Switched On Computing' scheme of work that the school have adopted, and will cover the use of technologies safely when both in school and at home.
- Regular whole assemblies are held by the Computing coordinator / senior staff to highlight the importance of e-safety and the latest risks.
- Failure to adhere to the policy will result in the pupil's access to the internet/ computing resources being removed.
- An annual 'e-safety' activity will be held in all classes across KS1 and KS2 where all aspects of safety will be covered relevant to the age of the pupils.

- School will access Community Police Officers for Y6 Training on Keeping Safe to cover e-safety in summer term annually.
- Pupils will be given a copy of the Pupil Acceptable Use Agreement (Appendix 1).

Introducing the policy with staff

- All staff in school will be given the School e-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Staff will be asked to read and sign a copy of the Acceptable Use Agreement (Appendix 2).

Discretion and professional conduct is essential.

- Training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

Parents' support

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- We will make use of parents' expertise for staff training, children's lessons and strategic direction should there be an identified need and suitable parental support / expertise.
- At Asterdale we have had addressed incidents of Cyberbullying, inappropriate use of the internet as well as identifying where children have been targeted and "groomed" over recent years. We have addressed these successfully with parents and external services. We ensure our focus is child centred and is supportive of the child who is vulnerable; we do so sensitively but effectively.

Appendix 1

Asterdale E-Safety Rules

Pupil Acceptable Use Agreement

- I will only use ICT in school for school purposes.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.
- I will not use a personal mobile phone, IPad, tablet or any other personal mobile device during school hours.
- If I bring any personal mobile device into school, I will hand it to my teacher at the beginning of school and collect it at home time.
- I understand that the school is not responsible for any personal ICT equipment brought into school.

Appendix 2

Acceptable use Agreement for Staff

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher or the Chair of Governors.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorized by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the head-teacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes online with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature …….…… Date ……

Full Name ……..... (printed)

Job title ……