On-line/E-Safety policy

Online safety now covers the safety issues associated with all information systems and electronic communications. This encompasses not only the internet but all wireless electronic communications including mobile phones, games consoles, cameras and webcams. It also takes into account the increasing mobility of access to digital technology through the range of mobile devices. At Willow Brook we recognise that the issue at hand is not the technology but the behaviour around how we use it; the use of new technologies in education brings more benefits than risks.

We aim to ensure that our young people are able to use the internet and related communications technologies appropriately and safely and this is part of the wider duty of care to which all who work in our school are bound.

Through this policy, we aim to meet our statutory obligations to ensure that our pupils are safe and are protected from potential harm, both within and outside school. We recognise that our online safety practices are also now part of our additional duties under the Counter Terrorism and Securities Act 2015 which requires all schools to ensure that children are safe from terrorist and extremist material on the internet.

Policy development

This online-safety policy relates to other policies including those for Anti-bullying and Child Protection.

- Our policy has been agreed by senior managers and approved by governors.
- The policy and its implementation will be reviewed at least once a year but will be flexible enough to respond to any significant new developments.
- It is available to read or download on our school website or as a paper copy from the school office.

Roles and responsibilities

The school has an e-safety coordinator. Our coordinator is the head teacher in their capacity as senior designated officer. Jamie Jones, as the lead teacher for Computing, has a responsibility to promote this policy and ensure it is reflected in teachers' planning and practice as well as their professional development. A link governor is nominated to monitor the implementation of the policy. We recognise that for an Online Safety Policy to succeed it must be owned and accepted by the whole school community.

Teaching and Learning

Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact.
- Issues such as Cyberbullying and e-safety are built into the curriculum to encourage self – efficacy and resilience. Specific units of direct teaching, as well as instilling regular safety reminders, will continue to inform and enable children to develop safe online habits. Some children who have experienced problems or with additional needs may need additional support.

Managing Internet Access
Information security system

- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Atom IT will provide alerts in respect of unauthorised access and suspicious on-line activity in line with our Keeping Children Safe in Education and Prevent duties. Appropriate and prompt responses will be made to these alerts.

Email

- Pupils and staff may only use approved e-mail accounts on the school system
- Pupils must immediately tell a member of staff if they receive offensive e-mail.
- Staff to pupil e-mail communication must only take place via a school e-mail address or from within a learning platform and will be monitored
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the school's website should be the school address. No staff or pupil's personal details should be published
- The headteacher or their nominee will have overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified.
- Pupil's full names will be avoided on the website and learning platforms including blogs, forums especially if associated with a photograph.
- Written permission will be obtained from parents and carers before photographs are published on the school website
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing

- The school will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site; it may need monitoring and educating students in their use.
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.

Managing filtering

- The school will work with the County Council to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material should be reported to the e-safety manager
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions.

Managing video conferencing

- Video conferencing will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving a video conference call.

Managing Emerging Technologies

- The school will examine emerging technologies for their educational benefit
- Personal mobile phones and associated cameras will not be used by staff in lessons or formal school time except in the event of an emergency.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required on site during the school day.
- Whilst pupils in Year 6 are permitted to bring mobile phones to school with permission, these will be switched off and stored during the school day. Pupils will not be permitted to use these without adult supervision on the school premises.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Policy decisions

Authorising internet access

- All staff must read and sign the 'staff code of conduct' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are given access to school IT systems.
- Pupils' access to search engines on the internet will be by adult demonstration or with directly supervised access to specific materials. Where possible, staff will prepare links to appropriate online sites for lessons. Children are not permitted to use personal mobile phones with internet access in school.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to regularly establish that the e-safety policy is appropriate and effective.
- Senior leaders will ensure that all staff keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Complaints of misuse by staff will be referred to the headteacher
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the schools behaviour policy.

Community use of the internet

- All use of the school internet connection by other members of the community shall be in accordance with the e-safety policy and with the knowledge of the headteacher or governors.

Communicating the policy

Pupils

- Appropriate elements of the online policy will be shared with pupils
- E-safety rules will be posted in all networked rooms
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff

- The e-safety policy is accessible within all classrooms.
- Staff should be aware that the system is monitored and that professional standards are expected.
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting

Parents

- The school will take every opportunity to help parents understand online issues through parents' evenings, newsletters, letters, website articles and information about national/local online safety campaigns/literature
- Parents will be notified of the policy on the school website
- Parents will be reminded of the school's policy on the use of photographs and social media when attending events.
- All parents will be asked to sign the Home School Agreement when they register their children.

This E-safety policy was revised by: Louise Ballard
In: February 2017
Review: February 2018