Christ Church C of E Primary School
E-Safety Policy

Our e-safety policy has been written by the school, based on guidance from BECTA and NTGfL. It has been agreed by the senior leadership team and approved by governors following discussions with parents and pupils. It will be reviewed annually.

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the schools' management, information and management systems.

How does the Internet benefit education?

- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils and staff
- Staff professional development through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Improved access to technical support
- Exchange of curriculum and administration data with LA and DFES

How will Internet use enhance learning?

- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval.

How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites, The URL (address) and content must be reported to the ICT technician
- Staff and pupils should ensure that their use of Internet derived materials complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and show how to validate information before accepting it's accuracy
- Pupils will be taught to acknowledge the source of information used and to respect copyright.

How will e-mail be managed ensuring safety for pupils and staff?

- Pupils and staff may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Staff must immediately tell a member of SLT if they receive offensive e-mail
- Pupils must not reveal details of themselves or others in e-mail communication or via a personal web space, such as their age, the location of the school, messaging account details, an address or telephone number, or arrange to meet anyone.
- Personal e-mail or messaging between staff and pupils should not take place
- The forwarding of chain letters is not permitted

How should website content be managed?

- The point of contact on the website will be the school address, school e-mail and telephone number. Staff home information will not be published
- Website photographs will be carefully selected and will only show pupils whose parents have given permission for their photographs to be used
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- The ICT Co-ordinator with the support of the staff and governors at Christ Church are responsible for monitoring the content of the school website, ensuring that material uploaded is appropriate, used with permission and up to date.

Newsgroups, e-mail lists and forums

- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated
- Access to forums that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted

Chat and Instant Messaging

- Pupils will not be allowed access to public or unregulated chat rooms
- Pupils will not access social networking sites for example 'Facebook' 'My Space' or 'Bebo'
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised
- Any form of bullying or harassment is strictly forbidden
- A risk assessment will be carried out before pupils are allowed to use a new technology in school

Extremist material and radicalisation

- We ensure that all staff and children are kept safe from terrorist and extremist material when they are in school through the filters provided by the local authority.
- If there are any incidences of suspicions of radical material being present on school systems they will be reported immediately to a senior member of staff or the headteacher.
- Any further information required please refer to the Christ Church C of E Primary School Tackling Extremism & Radicalisation policy

Personal websites and blogs

- When publishing materials to websites and elsewhere, pupils should consider the thoughts and feelings of those who might view the material. Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable

Photographic, video and audio technology

- Care should be taken when capturing photographs or videos to ensure that all pupils are appropriately dressed
- Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities.

- Pupils should always seek the permission of their teacher before making audio or video recordings within school.
- Pupils should not post photos of pupils wearing school uniform or any of staff
- Inappropriate material should not be downloaded onto school hardware

How can emerging ICT applications be managed?

- 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. Any phone brought into school must be stored in a central location in the school office.
- The sending of abusive or inappropriate text messaging is forbidden
- Mobile phone cameras should not be used inappropriately and photographs should not be forwarded to unknown sources
- Use of blog messaging sites such as the school Twitter account will be closely monitored by an adult at all times.

How will risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the 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 North Tyneside Council can accept liability for the material accessed, or any consequences of Internet access.
- 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.
- Access is strictly forbidden to any websites that involve gambling, games, financial scams, pornography and adult material.

How will filtering be managed?

- The school will work in partnership with parents, the LEA and DFES to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, The URL (address) and content must be reported to the ICT technician.
- SLT will ensure 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 referred to the Internet Watch Foundation (www.iwf.co.uk)

How will the policy be introduced to pupils?

- Rules for Internet access will be posted in all rooms where computers are used
- Pupils will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede internet access
- A module on responsible Internet use will be included in the ICT curriculum coverage covering both home and school use

How will staff be consulted and made aware of this policy?

- All staff must accept the terms of the 'Acceptable Use Policy' statement before using any internet resource in school
- All new staff will be taken through the key parts of this policy as part of their induction
- All staff including teachers, learning support assistants and support staff will be provided with the School e-Safety Policy and have its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible internet use, and on the school Internet policy will be provided as required
- Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security
- Virus protection will be installed and updated regularly
- Personal data sent over the internet will be encrypted or otherwise secured
- Use of portable media such as memory sticks will only be through school provided encrypted media.
- Files held on the school network will be regularly checked

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a member of the Senior Leadership Team
- Any complaint about staff misuse must be referred to the Head Teacher
- Pupils and parents will be informed of the complaint procedure
- Parents and pupils will need to work in partnership with staff to resolve issues
- As with drug issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention will be drawn to responsible Internet use in newsletters, and on the school website
- Internet issues will be handled sensitively to inform parents without undue alarm
- A partnership approach will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Reviewed and written March 2017
Next review due March 2019