Yorkshire Causeway SCHOOLS TRUST

E-SAFETY POLICY

The safe use of ICT and the Internet

History of document: To be reviewed annually and re-approved every three years, or sooner if deemed necessary.

Issue number	Author	Date written	Approved by Board	Comments
1	C Burt	Sept. 2017	28/11/2017	

Introduction

This document is a statement of the aims, principles, strategies and procedures for the use of Information and Communications Technology (ICT) throughout the Trust and its schools. It also recognizes the risks involved in both existing and new/emerging technologies.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.
- National Education Network standards and specifications.

The distinctive contribution of Information and Communication Technology to the school curriculum.

Information and Communication Technology (ICT) contributes to the curriculum by preparing all students to participate in a rapidly changing society in which work and other forms of activity are increasingly dependent on ICT. The subject develops students' information skills, including the ability to use information sources and ICT tools to help them find, explore, develop, analyse, exchange and present information and to support their problem solving, investigative and expressive work. An essential part of ICT capability is evaluating information and the ways in which it may be used, and making informed judgements about when and how technology can be used. Students also develop understanding of the implications of ICT for working life and society. The use of ICT significantly enhances teaching and learning in other subjects by enabling rapid access to knowledge, information and experiences from a wide range of sources. The use of ICT throughout the curriculum encourages critical thinking, imagination and creativity, problem solving, initiative and independence, teamwork and reflection.

The addition of Computing to the curriculum allows pupils the opportunity to create digital technology and software for themselves and gives them an understanding of how the systems that they use work; therefore making students better informed and more responsible users.

Aims

Through the use and teaching of ICT/ Computing the Trust aims to:

- Meet current requirements of Curriculum.
- Help other curriculum areas meet the requirements of curriculum change through the support of ICT.
- Allow staff and students to gain confidence in, and enjoyment from, the use of ICT and Computing.
- Allow students to develop specific ICT and Computing skills as set down in a school's scheme of work.
- Ensure that staff and students alike understand the capabilities and limitations of ICT and gain insight into the implications of its development for society.
- Allow teaching staff to develop professionally by enhancing their teaching skills, management skills and administrative skills.
- Support all trainee teachers in their use of ICT in the curriculum as part of their Initial Teacher Training.

Authorised Internet Access

- All students, staff and visitors must read and sign a Computer Network and ICT Acceptable Use Agreement before using any school ICT resources.
- Parents will also be asked to sign and return the Student Computer Network and ICT Acceptable Use Agreement.
- The Trust/Schools will maintain a current record of all staff and students who are granted Internet access.
- Parents will be informed that students Internet access will be monitored and that it is not possible to filter all unsuitable sites.
- Students must apply for Internet access individually by agreeing to comply with the Computer Network and ICT Acceptable Use Agreement.
- Access to the wi-fi in each school will be managed locally, by each school, through the use of specific log on and passwords available from the IT Office/Headteacher/Administrator.

World Wide Web

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the ICT Network Team/Relevant Class Teacher.
- All teaching staff should ensure that their use of Internet derived materials, and that of students, complies with copyright law.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive any offensive e-mails.
- Students must not reveal personal details of themselves, or others, in e-mail communications, or arrange to meet anyone, without specific permission.
- Staff should not disclose any personal details about themselves when communicating via email with students.
- All communication with students should be through the school email system and not through staff members or students' personal email accounts. Access in school to external personal e-mail accounts may be blocked.
- Any Email sent from the school should be written with the same considerations as a letter written on school headed paper and follow exactly the same procedures and protocols.

Social Networking

- The School will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students should be advised not to place personal photos on any social network space.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Filtering

- The Trust will be using a professional, versatile proxy server that filters Web content using a number of techniques. These include real-time context analysis in multiple languages, a known database of categorised sites and sophisticated image content analysis.
- The Trust uses SSL Intercept Mode. This means every time you visit a site in the form https://somesite.com the Smoothwall software will decrypt, check and re-encrypt the traffic before continuing communication with the target site*.*
- As students progress through school they are given greater responsibility as the filtering of internet use is reduced. Sixth Formers for example have access to YouTube to allow them to access its many educational resources.

Computer monitoring

- The Trust's firewall monitors traffic to the web and produces a daily printout of potential inappropriate searches using keyword monitoring. These reports are reviewed on a regular basis by a member of the Senior Leadership Team.

Video Conferencing

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies including Tablet Computers & Mobile Telephones

- 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 for personal use during lessons or formal school time (student's mobile phones should normally be switched off and out of sight during lesson time). However, the teacher in charge may give permission for the use of mobile phones for educational purposes.
- The sending of abusive or inappropriate messages in all forms, and using all technologies, is forbidden.

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or students' personal information will not be published.
- The Trust will adopt a Publication Scheme in line with Information Commissioner guidance.

Publishing Students' Images and Work

- Photography and Video: Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, must always be sought before an image is published for any purpose. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet.
- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will not be used anywhere on Trust Websites, Blogs or any Social Media content, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or video of students are published on the school Web site.
- Work can only be published with the permission of the student and parents.

Information System Security

- Trust ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with all stakeholders.
- Laptops (supplied by the school for teachers) should be connected to the school network at least once per calendar month to allow for anti-virus scans / updates to occur and software updates to be installed.
- Access to USB memory sticks is disabled.

Internet Danger Awareness

All teaching staff and all Students will be made aware of the potential dangers of online activity and trained in Internet safety under the ThinkUKnow scheme by CEOP as a minimum.

A program of E-safety education will be delivered throughout the year covering cyberbullying, sexting, using ICT in the workplace and digital footprints. These messages are supplemented and reinforced by assemblies.

Parents will be alerted to topical issues relating to internet danger by emails and newsletters.

Protecting Personal Data

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

Assessing Risks

The Trust will take all reasonable precautions to prevent access to inappropriate material.

However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The Trust, therefore, cannot accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Access to inappropriate images and Internet usage

There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

Adults should not use equipment belonging to the Trust to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children. School equipment can be monitored to guard against inappropriate usage.

Adults should ensure that children and young people are not exposed to any inappropriate images or web links. Organisations and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. E.g. personal passwords should be kept confidential.

Where indecent images of children or other unsuitable material are found, the Designated Safeguarding Lead (DSL) or Child Protection Officer (CPO) should be immediately informed (depending on material / circumstances the police and Local Authority Designated Officer (LADO) may also be informed). Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

Risks to students from the internet and emerging technologies

Some of the more common risks to children and young people, which all users need to be aware of, and which the Trust staff will be actively monitoring and looking for signs of are:

Children/students viewing adult pornography.

Children/students abused through using the internet and mobile phones.

Children/students creating and sending indecent images of themselves to others.

Children/students who create, view or download sexually abusive images of other children.

Children/students creating or placing images of other children online.

Children/students groomed for sexual abuse online.

Children/students made the subject of child abuse images or pseudo-images.

Inappropriate material promoting sexual/racial intolerance and/or terrorism/extremist behaviour.

Prevent Duty responsibilities

In cases of potential radicalisation/extremism the national Prevent Duty may be implemented which could lead to the referral of individuals to the Prevent Duty Delivery Board and the Channel Panel in specific circumstances.

The objectives of the Prevent strategy are to:

- Respond to the ideological challenge of terrorism and the threat faced from those who promote it
- Prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support
- Work with sectors and institutions where there are risks of radicalisation that need to be addressed

The guidance from the Home Office explains that schools should be "safe spaces" that allow pupils to "understand and discuss sensitive topics" such as terrorism and extremist ideas, and enable pupils to challenge these ideas.

It adds:

The Prevent duty is not intended to limit discussion of these issues.

Schools should, however, be mindful of their existing duties to forbid political indoctrination and secure a balanced presentation of political issues.

Cyber-bullying.

This can take many forms and has the potential for a much wider audience by its very nature and, as a result, a much greater level of participation. All incidents of cyberbullying will be recorded by the school and pupils will be made aware of how to report such incidents. Internet access and the use of ICT equipment will be restricted to anyone guilty of cyberbullying, with parents/carers involved as appropriate.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by the Network Managers and/or schools Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Communication of Policy

Students

- Rules for Internet access are posted in all ICT suites.
- Students will be informed that Internet use will be monitored.
- Advice and e-safety information available to students via School Websites and Intranet (under "E-Safety" link).

Staff

- All staff will be given the School e-Safety Policy and 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 that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Parents

- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the Trust/School Web site.
- Advice and e-safety information will be available to parents via Trust/School website (under "ESafety" link).
- Parents should be aware that the Trust will take any reasonable action to ensure the safety of its students: in cases where the school has reason to be concerned that any child may be subject to ill-treatment, neglect or any other form of abuse, the school has no alternative but to follow the Trust's Child Protection Policy.