Online 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.

Version	Author	Date written	Approved	Note of key revisions
V1	C. Burt	Sept. 2017	28 Nov. 2017	
V2	L. Claringbold	08 Dec. 2020	26 Jan. 2021	Clause 7 inserted re: Equipment
V3	L. Claringbold	16 Sep. 2021	05 Oct. 2021	Updated to reflect the online safety additions to KCSIE 2021

Contents

1. 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.

Online Safety encompasses internet technologies and electronic communications such as mobile phones and smart 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.

Online 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 online 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.

1.1. The distinctive contribution of ICT 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.

1.2. 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.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors, with clear mechanism to identify, intervene and escalate incidents, where appropriate.

1.3. Online safety - The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk as defined in Keeping children safe in education 2021[1] (KCSIE):

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014057/KCSIE_2021_September.pdf

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Roles and responsibilities

2.1. The trustees

The trustees have overall responsibility for setting and monitoring this policy and, for gaining assurance of its implementation.

2.2. The governing board

The governing board has a responsibility for monitoring this policy and holding the headteacher to account for its implementation

The governing board will co-ordinate regular meetings with staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils of SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

2.3. The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

2.4. The designated safeguarding lead (DSL)

Details of the school's DSL are set out in our child protection policy. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy, ensuring all incidents are logged and dealt with appropriately

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

2.5. The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed with the DSL and updated on a regular basis with the DSLs to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online, while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately

This list is not intended to be exhaustive.

2.6. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing the policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety are logged and dealt with appropriately
- Ensuring that any incidents of cyberbullying are dealt with appropriately and in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of "it could happen here"

This list is not intended to be exhaustive.

2.7. Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

- Healthy relationships – Disrespect Nobody

2.8. Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, where relevant, and expected to read and follow it. If appropriate they will be expected to agree to the terms on acceptable use.

3. Authorised internet access

3.1. General

- 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.

3.2. 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.

3.3. 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.
- School email accounts should not be used to register for any type of non-school related online account (including all forms of social media) without express permission from the ICT Network Team/Headteacher.

3.4. 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.

3.5. Filtering and monitoring

- 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 filter 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 may have access to YouTube to allow them to access its many educational resources dependent on what courses they are on.
- The Trust's firewall monitors traffic to the web and produces a daily report of potential inappropriate searches using keyword monitoring. These reports are reviewed on a regular basis by a member of the Senior Leadership Team.

3.6. 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.

4. 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.

5. Published content

5.1. School website

- 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.

5.2. 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.

6. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998[2].

7. 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.

8. Equipment

Staff should not use personal laptops/tablets for school related activities. Where this is unavoidable, then you should seek permission from the ICT Network Team and the following preventative steps taken:

- Due care and attention should be taken to protect usernames and passwords. You should never use 'remember me' to store any usernames or passwords, particularly on personal equipment.
- Software such as Teams should be logged off at the end of each session in order to prevent unauthorised/accidental access.
- No school related data/information should be downloaded and stored onto personal laptops.

[2] https://www.legislation.gov.uk/ukpga/1998/29/contents

9. 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[3] scheme by CEOP as a minimum.

A program of online 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.

10. 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 online safety policy is adequate and that the implementation of the online safety policy is appropriate.

10.1 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.

[3] https://www.thinkuknow.co.uk/

10.2. 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.

10.3. 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[4] 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.

11. 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.

[4] https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales

12. Handling online safety complaints

- Complaints of internet misuse will be dealt with by the Network Managers and/or school's 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.

13. Communication of policy

13.1. Students

- Rules for internet access are posted in all ICT suites.
- Students will be informed that internet use will be monitored.
- Advice and online safety information available to students via School Websites and Intranet

13.2. Staff

- All staff will be given the School Online 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.

13.3. Parents

- Parents' attention will be drawn to the School Online Safety Policy in newsletters and on the Trust/School Web site.
- Advice and online safety information will be available to parents via School website).
- 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.

Associated policies

Below are listed the associated policies for consideration when reading and reviewing this policy:

- YCST Acceptable Use Agreement (Adult/Student/Visitor)
- School Child Protection Policy
- Behaviour Policy
- Anti-bullying Policy