St. Cuthbert's R.C.
Primary School Hartlepool

ICT Acceptable Use Policy (E-Safety)	
Reviewed: -	December 2019
Next review: -	December 2021
Author: -	
Hartlepool Education Authority / J.M. Wilson	

ICT Acceptable Use Policy (E-safety)

Mission Statement **"Let the light of Christ shine in us all."**

BACKGROUND AND RATIONALE

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times. The requirement to ensure that children and young people are able to use the internet and related communications technologies safely is addressed as part of the wider duty of care to which all who work at St Cuthbert's Primary are committed to. The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site. This is pertinent to incidents of cyber-bullying or other E-Safety incidents which may take place out of school, but are linked to school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate E-Safety behaviour that take place out of school. While developing technology brings many opportunities, it also brings risks and potential dangers. This policy demonstrates how we strive to keep children safe with technology whilst they are in school. We also recognise that children are often at risk when using technology at home [where we have no control over the technical structures put in place to keep them safe] and so this policy sets out how we educate children about the potential risks through good provision, to build pupils' resilience and knowledge, so that they have the confidence and skills to face and deal with these associated risks. St Cuthbert's E-Safety policy applies to all members of the school community [including staff, pupils, volunteers, parents/carers, governors and visitors] who have access to, and are users of, school ICT systems, both in and out of school. It must be fully complied with at all times and is monitored on a regular basis.

ROLES AND RESPONSIBILITIES

At St Cuthbert's School we have an E-Safety team which reviews and advises on our policies. The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school.

Headteacher

- The Headteacher is responsible for ensuring the safety [including E-Safety] of all members of the school community, though day-to-day responsibility for E-Safety will be delegated to the E-Safety Coordinator.

- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive appropriate PD to enable them to carry out their E-Safety roles as relevant.
- The Headteacher and Deputy Head [In the Head's absence] are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.
- The Headteacher is responsible for supporting the E-Safety Coordinator in creating an internet safety culture within the school, including speaking to staff and pupils in support of the programme.
- The head teacher is responsible for ensuring that the governing body is informed of the issues and the policies.

Governing Body

- Governors are responsible for the approval of the E-Safety policy and for reviewing the effectiveness of the policy.

E-Safety/Computing Coordinator

- Takes day-to-day responsibility for E-Safety issues and has a leading role in establishing and reviewing the policy.
- Ensures that the ICT infrastructure is secure and is not open to misuse or malicious attack through liaising with One-IT and checking whether there have been any breaches with One-IT.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident.
- Provides PD and advice for staff.
- Liaises regularly with Senior Leadership Team.

Class Teachers

- They have an up to date awareness of E-Safety matters and of the current school acceptable use policy and practices.
- They have read and understood the Acceptable Use Policy.
- They report any suspected misuse or problem to the E-Safety Leader for investigation/sanction/action.
- Digital communications with pupils should be on a professional level and only carried out using official school systems
- Pupils understand [as appropriate to their age] and follow the school E-Safety practices
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They embed E-Safety issues in the curriculum and other school activities

ICT Technician is responsible for ensuring that:-

- The school's ICT infrastructure and data are secure and not open to misuse or malicious attacks, alongside the E-Safety Leader.
- Shortcomings in the infrastructure are reported to the ICT Leader or Headteacher so that appropriate action can be taken.

Designated Person- Child Protection

Our Designated Person (Child Protection) – Mrs. J M Wilson is the first point of contact for any Internet safety issue, which may compromise the wellbeing of a pupil, and as such, they are involved in: -

- Seeking professional development on the safety issues relating to use of the Internet and related technologies, and how these relate to children and young people, refreshing this knowledge on a regular basis.
- Acting as a key member of the school's E-Safety leader providing follow-up counselling and support to both victims and perpetrators as appropriate.
- Taking a proactive role in the Internet safety education of pupils.
- Developing systems and procedures for supporting and/or referring on pupils referred to them as a result of breaches of Internet safety within schools.
- Developing relationships with colleagues at LA level (including counsellors and guidance staff) and other organisations that can provide advice, referrals or resources on issues relating to child protection on the Internet.

Pupils

Our ultimate aim is for pupils to take responsibility for their own actions when using the Internet and other communications technologies, with each pupil developing a set of safe and discriminating behaviours to guide their own Internet use. Responsibilities we promote are:-

- Upholding school policies relating to acceptable use of the Internet and other communications technologies.
- Developing their own set of safe and discriminating behaviours to guide them whenever they are online and to produce a leaflet in 'Child Friendly' language.
- Reporting any incidents of ICT misuse within school to a member of the teaching staff.
- Seeking help or advice from a teacher or trusted adult if they experience problems when online or if they receive any content or contact which makes them feel uncomfortable in any way.
- Communicating with their parents or carers about Internet safety issues, and upholding any rules for safe Internet use in the home.

UNSUITABLE/INAPPROPRIATE ACTIVITIES

Some internet activity, e.g. accessing child abuse images or distributing racist material, is illegal and is obviously banned from school and all other ICT systems. Other activities, e.g. Cyber-bullying, is and could lead to criminal prosecution. The school believes that the activities listed below are inappropriate in a school context and that users should not engage in these activities in school or outside school. The school policy restricts certain internet usage as follows:-

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:-

- Child sexual abuse images.
- Promotion or conduct of illegal acts e.g. under the child protection, obscenity, computer misuse and fraud legislation.
- Adult material that potentially breaches the Obscene Publications Act in the UK;
- Criminally racist material in the UK.
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial, religious or homophobic hatred.
- Accessing websites which promote religious extremism or radicalisation.
- Threatening behaviour, including promotion of physical violence or mental harm;
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the school:-

- Using school systems to undertake transactions pertaining to a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information [e.g. financial/personal information, databases, computer/network access codes and passwords].
- Creating or propagating computer viruses or other harmful files.
- On-line gambling and non-educational gaming.

RESPONDING TO INCIDENTS OF MISUSE

All members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In such cases, the following procedures should be followed:-

- If a pupil or member of staff accidentally accesses inappropriate or illegal material, the ICT device display should be switched off, but the device should not be shut down. It may also be appropriate to disconnect the device from the school network. The teacher in charge of the class should then inform the E-Safety coordinator and/or the Head teacher. The incident will then be dealt with in a proportionate manner.
- If a pupil suspects that someone is deliberately accessing inappropriate or illegal material, he/she should speak to his/her class teacher [unless it is the class teacher that the pupil suspects] or any other adult that he/she trusts. This adult should then inform the Headteacher.
- If a member of staff suspects that someone is deliberately accessing inappropriate or illegal material, he/she should inform the Head teacher [or Deputy Headteacher if the member of staff suspects the Headteacher] Sanctions are as follows:-

- In the case of a pupil deliberately accessing inappropriate materials, sanctions will be imposed by the Headteacher in line with the child's parent[s]/carer[s].

- In the case of a pupil deliberately accessing illegal materials, sanctions will be imposed by the Headteacher in line with the child's parent[s]/carer[s] and criminal procedures will be followed.
- In the case of a staff member deliberately accessing inappropriate materials, sanctions will be imposed in line with the adopted School's Disciplinary and Capability Policy
- In the case of a staff member deliberately accessing illegal materials, criminal procedures will be followed.
- The E-Safety Coordinator will record all reported incidents and actions taken in the School on to CPOMS.
- The Designated Child Protection officer will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

MOBILE PHONES AND PERSONAL DEVICES

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis.

Children are not permitted to have or use mobile phones in school except for special one off occasions in which permission is sought and use is subject to school restrictions i.e. Timetables rock stars day.

Staff are permitted to use phones to record learning through photographs or videos however these must be downloaded and deleted from the phone before leaving the school premises. It is recommended that the schools iPads are used for this purpose to protect staff and children.

E-MAILS

All staff must use a school email for any information or messages being shared that are in relation to school. Personal email addresses must never be used for school related emails.

CYBERBULLYING

Cyberbullying [along with all other forms of bullying] of any member of the school community will not be tolerated. There are clear procedures in place to support anyone in the school community affected by cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence and this will be recorded on cpoms.
- The school will take steps to identify the bully, where possible and appropriate. This may include identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying subsequent consequences.
- the bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- internet access may be suspended at school for the user for a period of time.

- other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- parent/carers of pupils will be informed.
- the Police will be contacted if a criminal offence is suspected.

SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING

- 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, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- school official social media, blogs or wikis should be password protected and run with approval from the Senior Leadership Team.
- pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications • concerns regarding students' use of social networking, social media and personal publishing sites [in or out of school] will be raised with their parents/carers, particularly when concerning children's' underage use of sites.

USE OF DIGITAL AND VIDEO IMAGES

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment or downloaded before leaving school.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

WEBSITE

- St. Cuthbert's uses the public website http://www.stcuthbertsschool.org.uk/ for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of children. All users are required to consider good practice when publishing content.
- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff [never pupils].
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images.

PROFESSIONAL STANDARDS FOR STAFF COMMUNICATION

In all aspects of their work in St Cuthbert's School teachers follow the Professional Teaching Standards as described by the DfE: 7. Teachers translate these standards appropriately for all matters relating to E-Safety.

- Any digital communication between staff and pupils or parents / carers [email, chat, etc.] must be professional in tone and content.
- These communications may only take place on official [monitored] school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are also used to inform this process.

MANAGING INFORMATION SYSTEMS

The school through ONE-IT will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly • personal or sensitive data taken off site will be encrypted.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT/Computing Coordinator and Technical support will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

FILTERING

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School E-Safety Leader who will then record the incident and escalate the concern as appropriate
- The School filtering system will block all sites on the Internet Watch Foundation [IWF] list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The ICT Leader and Technician will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Hartlepool Police or CEOP E-SAFETY EDUCATION.

E-SAFETY EDUCATION WILL BE PROVIDED IN THE FOLLOWING WAYS

- Staying safe online messages and practice is embedded into the Computing curriculum.
- Key E-Safety messages will be reinforced through further input via assemblies, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand and encouraged to adopt safe and responsible use of ICT both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

STAFF TRAINING/STAFF DISCUSSION

It is essential that all staff including non-teaching staff receive E-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:-

- E-Safety training will be made available to staff. An audit of the E-Safety training needs of all staff will be carried out regularly.
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, and others.
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for input to parents, is sought from External agencies when appropriate. (i.e. Safety newsletter)
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

PARENT AND CARER AWARENESS RAISING

Many parents and carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". [Byron Report]. The school will therefore seek to provide information and awareness to parents and carers through: letters, newsletters and the school website.

Appendix 1

Flowchart for Primary Schools