Castle Tower School

E-Safety Policy

Context

This policy is based on and complies with DENI circular 2007/1 on Acceptable Use of the internet, Digital Technologies in schools and DENI circular 2011/22 on internet safety and DENI circular 2016/27 on online safety.

The above circulars states that 'used well digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices, is a key goal for schools.'

Information and Communications Technology in Castle Tower School is concerned with the use of hardware, software and peripherals to provide our pupils with a broader and more accessible curriculum. ICT is intended to encourage pupils to make individual responses and use technology appropriately. ICT contributes to all subject areas supporting and extending the work already being carried out - it is an important and integral part of the learning and teaching process.

Care and Responsibility

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. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. With these opportunities we also have to recognise the risks associated with the internet and related technologies.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement

- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

As with all other risks, it is impossible to eliminate the risk completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with any scenarios which may arise. In Castle Tower School we understand the responsibility to educate our pupils in E-Safety issues. We aim to teach pupils appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities
As E-Safety is an important aspect of Child Protection within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current E-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of E-Safety throughout the school. The Principal/ICT Co-Ordinator have the responsibility to update Senior Management and Governors with regard to E-Safety and all governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice.

E-Safety Skills Development for Staff
- All staff with reference to this policy will be aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff members have access to the E-Safety policy via Fronter.
- All staff are encouraged to incorporate E-Safety into their activities and promote awareness within their lessons.

Handling of E-Safety Issues
Issues of Internet misuse and access to any inappropriate material by any user should be reported to the ICT Co-ordinator to be recorded. Issues of a child protection nature will be reported to the designated teacher and dealt with in accordance with the Castle Tower School Child Protection Policy. Incidents of pupil misuse of technology which arise will be dealt with in accordance with the school's behaviour policy.

E-safety and pupils
E-safety will be discussed with pupils at the start of the year when they receive their Acceptable Use Agreement. This should be discussed as a set of rules that will keep everyone safe when using technology in school.

Activities throughout the school year including School Assemblies, Internet Awareness Day and visits from the PSNI will refresh E-Safety and further pupils' understanding.
Pupils will be informed that all network and Internet use is monitored.

E-Safety and Parents
Parents will be required to read the Acceptable Use Agreement for pupils and sign this agreement following discussion with their child.

E-Safety and Staff
All staff will be introduced and directed to the E-Safety policy on Fronter. Staff will be asked to read and sign the Acceptable Use Agreement for Staff which focuses on E-Safety responsibilities in accordance with the Code of Conduct for employees set out in the Staff Handbook .Staff should be aware that all Internet traffic and email is monitored, recorded and tracked by the C2K system.

The Internet
The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials, some of which could be unsuitable.

Networks
Pupil access to the Internet is through a filtered service provided by C2K, which should ensure educational use made of the resources is safe and secure, protecting users and systems from abuse.
Use of a C2K wireless network for use with iPads in school is provided by an external Internet provider. This network has appropriate filters applied for use by staff and pupils and use of iPads will only be carried out under staff supervision.
Connection of mobile phones or personal computers to the wireless network is not permitted for pupils.

Teaching and Learning
Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school will be discussed with pupils.
- Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/guardian, teacher/trusted member of staff.
- The school Internet access is filtered through the C2k managed service.
- Use of the internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.
- Children will be taught to be 'Internet Wise'. They will be made aware of Internet Safety Rules and encouraged to discuss how to cope if they come across inappropriate material.

E-mail:

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children will not always be given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way will be supervised by the teacher.

School Website

The School website promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life.

In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff
- Permission to use pupil photographs on the website is requested each school year.

Social Networking:

- The school C2k system will block access to social networking sites.
- Social networking is not permitted during school.
- Our pupils are asked to report any incidents of cyber-bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

Password Security

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

Mobile Phones
School does not allow the use of mobile phones by children in school or on school trips.

Pupils are not allowed to use a mobile phone, tablet or any other mobile device in school unless I have been given permission by a teacher. If this rule is broken the device is to be handed into the school office and can only be collected by a parent/carer.

It is important to be aware of the safety issues regarding mobile phones which now increasingly have Internet access. Staff use of mobile phones, only when necessary, should be discreet. Mobile phones should not be used in the classroom setting and should not be visible to pupils throughout school.

iPad / Tablet Devices
The Mobile Technology policy, procedures and information applies to all iPads, or any other IT handheld device used in school. Teachers and other school staff may also set additional requirements for use within their classroom.

For more information please refer to the Mobile Technology Policy.

Policy updated March 2018

Castle Tower School
Acceptable Use of the Internet for Pupils

Parent/Carer

We strongly believe that children should know that they are responsible for their use of the Internet in school and that they do so in a safe and appropriate manner. Please discuss these guidelines with your child and stress the importance of safe use of the Internet. Please complete the reply slip attached and send it to school at your earliest convenience. Keep this sheet in the Home/School Information Pack you received at the start of the year for future reference.

As a pupil:

When using School Computers:

- I will only use my own username and password
- I will keep my username and password private
- I will not access other people's files without their permission
- I will not change or delete other people's work/files
- I will only use the Internet for school work
- I understand that all my documents can be accessed by school at anytime

Emails:

- I will only send e-mails in school when I have my teacher's permission. I will always make sure that the messages are polite and responsible, and I will not use strong language or swear words
- I will never give my name, address or phone number or arrange to meet anyone

Social Networks

- I am not allowed to enter social networking sites while in school
- If I see anything I am unhappy with or receive messages I don't like, I will tell a teacher immediately

Mobile Phones/Tablets ETC

- I am not allowed to use a mobile phone, tablet or any other mobile device in school unless I have been given permission by a teacher. If this rule is broken I understand that my device will be handed into the school office and can only be collected by my parent/carer
- I am not allowed to take photographs or videos in school unless I have been given permission by teacher

I understand that if I deliberately break these rules I could be stopped from using Computers in school and my Parent/Carer will be informed.

Castle Tower School
Acceptable Use of the Internet for Pupils

Reply slip for Acceptable Use of the Internet

I understand that if I deliberately break the rules above that I could be stopped from using Computers/Mobile Devices in school and my Parent/Carer will be informed.

Signature of Pupil: _____

Signature of Parent/Carer: _____

Date: _____

Castle Tower School
Acceptable Use of the Internet for Staff

Acceptable Use Agreement for Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's ICT and e-Safety policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- All Internet activity should be appropriate to staff professional activity or the pupils' education
- Access should only be made via the authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden
- Please be aware that school can access any documents stored on the C2k network at any time without the users permission

Name: _____

Signed: _____

Date: _____