The Castle School
A SPECIALIST COLLEGE FOR COMMUNICATION & INTERACTION

E-Safety Policy

What is E-Safety?

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to our students. Some examples of this are:

Bullying via chat or email
Obsessive internet use
Exposure to inappropriate materials
Inappropriate or illegal behaviour
Physical danger of sexual abuse

As a school it is our duty of care alongside that of parents and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this e-safety policy is to outline what measures The Castle School takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate manner.

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Students including those with Autistic Spectrum, need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be helped and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- E-safety should be taught in a way which is appropriate to the needs of each individual student. Those with ASC & communication difficulties and specific learning requirements such as the need for visual aids and structured teaching should be enabled to access E-safety education in an appropriate and accessible way.

Parents/Carers

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 / 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 Castle School will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
- Training and awareness sessions for parents and carers

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal 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
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.

Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of CPC subcommittee or who have responsibility for safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or National Governors Association
- Participation in school training / information sessions for staff or parents

Technical-infrastructure/equipment, filtering and monitoring

The school 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school systems are safe and appropriate for use by students.
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by West Berkshire.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to the network manager.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that students 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.
- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Use of digital and video images-Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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 eg on social networking sites.
- Staff are allowed to take digital / 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 taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data (including photographs), minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
    - the device must offer approved virus and malware checking software
    - data must be securely deleted once it has been transferred or its use is complete.

Use of equipment and communication technology in school

	Staff and other adults		Students	
	Allowed	Not allowed	Allowed	Not allowed
Mobile phones may be brought onto school site	X		X (must be given to class teacher)	
Use of mobile phones in lessons		X		X
Use of mobile phones in social time	X			X
Taking pictures on personal mobile phones		X		X
Use of personal email addresses in school or on school network		X		X
Use of school email for personal emails		X		X
Use of chat rooms		X		X
Use of instant messaging		X		X
Use of social networking sites		X		X
Use of blogs		X		X

When using communication technologies the school considers the following as good practice:
The official school email service may be regarded as safe and secure and is monitored.

- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Headteacher or member of the Leadership Team –the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE 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 programmes must not be used for these communications.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- **Unsuitable/inappropriate activities:** The school believes that the activities referred to in the following section would be inappropriate in a school context and users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The Castle School 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 (**Illegal**)
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer (**illegal**) misuse and fraud legislation (**Illegal**)
	adult material that potentially breaches the Obscene Publications Act in the UK (Illegal)
	criminally racist material in UK (**Illegal**)
	pornography
	promotion of any kind of discrimination
	promotion of racial or religious hatred
	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
	In addition, the following activities will not take place on the school site or network unless otherwise stated below:
Using school systems to run 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 (eg financial / personal information, databases, computer / network access codes and passwords) (**Illegal**)	
Creating or propagating computer viruses or other harmful files (**Illegal**)	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet	
On-line gaming (educational)	
On-line gaming (non educational)	
On-line gambling	

On-line shopping / commerce (Except by nominated staff)
File sharing with 3rd parties
Use of social networking sites

Responding to incidents of misuse from students:

Non-illegal activities: If any member of staff, adult or student believes that a student has been involved in any of the non-illegal activities above then, in the first instance this should be reported to the class teacher. The class teacher should then make a judgement as to what action is needed. The class teacher should ensure that the Key Stage Co-ordinator is made aware who will keep a record of the incident. Parents should be informed of the incident and, if appropriate invited in to discuss how to support them in the students use of internet at home.

Illegal activities: If any member of staff believes that a student has been involved in illegal internet use then this should immediately be reported to The Headteacher or The Deputy Headteacher (or member of the Leadership Team in their absence). The Headteacher or The Deputy Headteacher will instigate an investigation into the allegation.

Responding to incidents of misuse from staff:
It is hoped that 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.

It is important that any incidents of misuse are reported and dealt with quickly. If a member of staff feels that a member of school staff may have been involved in any of the above then they should report the issue to The Headteacher or The Deputy Headteacher immediately (or in their absence a member of the Leadership Team).

The following table shows what actions will be taken for different types of incident:

Staff	**Actions / Sanctions**							
Incidents:	*Refer to line manager*	*Refer to Headteacher*	*Refer to Local Authority / HR*	*Refer to Police*	*Refer to Technical Support Staff for action re filtering etc*	*Warning*	*Suspension*	*Disciplinary action*
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X			X	X		X
Unauthorised downloading or uploading of files		X			x	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x			X	X		X
Careless use of personal data eg holding or transferring data in an insecure manner	x				X	X		
Deliberate actions to breach data protection or	X	X			X	X		X

network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	X	X	X		X	X	X	X
Actions which could compromise the staff member's professional standing	X	X				x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				x		x
Using proxy sites or other means to subvert the school's filtering system		X			x	X		x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	X			X	x		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations		x			x	x		x
Continued infringements of the above, following previous warnings or sanctions		x						x

Rights Respecting Schools
This policy adheres to the principles of the United Nations Convention of the Rights of the Child (UNCRC) specifically articles: 1, 2, 3, 4, 5, 12, 14, 15, 16, 17, 18, 19, 23, 28, 29, 31, 34, 36 & 42.

Last review: 17 May 2018
Next review: May 2019