The Castle Partnership Trust
ACHIEVE | BELONG | PARTICIPATE

E-Safety Policy

Date: April 2016

Executive Headteacher: Sarah Watson
Headteacher, Court Fields School: Rachael Bennett

Lead Person: DHT

Contents

Background / Rationale

E-safety is part of the safeguarding duty of all those people who work in the schools and cannot be ignored or passed on to others.

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. Electronic communication helps teachers and students learn from each other. 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 appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The Castle Partnership Trust's e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy will involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student 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 materials
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with our other Trust policies (e.g. safeguarding, behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

We must as a Trust, demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The e-safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the Trust community (including staff, governors, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the Trust.

Where possible the Trust 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 safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors' Education Committee every two years.

Headteacher and School Leadership Team (SLT):

The Headteacher/SLT at each school is responsible for ensuring the safety (including e-safety) of members of the school community.

- Each Headteacher or a nominated member of SLT ensures that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Each Headteacher and the Business Manager or a nominated member of SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. See Somerset flow chart on dealing with e-safety incidents at http://tinyurl.com/3g4tmko

Network Manager / Technical staff:

The Network Manager is responsible for ensuring:

- That each school's ICT infrastructure is as secure as possible and is not open to misuse or malicious attack.
  - That each school meets the e-safety technical requirements outlined in the South West Grid for Learning (SWGfL) Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- SWGfL is informed of issues relating to the filtering applied by the Grid.
- That he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network/ remote access/email is regularly monitored in order that any misuse / attempted misuse can be reported using the guidance 'Responding to incidents of misuse'. And these incidents will be logged.
  - That monitoring software/systems are implemented and updated as agreed in Trust policies.

- Special procedures and Acceptable Use Policies (AUPs) will need to be signed to allow technical staff to explore issues concerning e-safety.

Teaching and Support Staff:

Are responsible for ensuring that

- They have an up to date awareness of e-safety matters and of the current Trust e-safety policy and practices.
- They have read, understood and signed the school Staff AUP.
- Staff will sign the AUP every year.
- Digital communications with students (email/voice) should be on a professional level.
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the Trust E-safety and acceptable use policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulation.
- They are aware of e-safety issues related to the use of mobile phones, cameras and mobile devices and that they monitor their use and implement current school policies with regard to these devices.
- Staff will record and log any incidents of e-safety according to school policies.

Designated person for child protection / Child Protection Officer:

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming

- Cyber-bullying
- Sexting
- Sexualized behaviour resulting from inappropriate internet use

Students:

- Are responsible for using their school ICT system in accordance with the student AUP.
  - Students will be expected to sign the AUP every year
  - Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
  - Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and mobile devices. They should also know and understand school policies on the taking/ use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the Trust's e-safety policy covers their actions out of school, if related to their membership of the school.

Parents / Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The Trust will take every opportunity to help parents understand e-safety issues through parents' evenings, newsletters, letters, website/VLE and the Parents' Voice Forum. Parents and carers will be responsible for:

- Accessing the school website/on-line student records in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, these 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 Trust's e-safety provision. Children and young people 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 and progressive e-safety programme will be provided as part of ICT lessons – this will cover both the use of ICT and new technologies in school and outside school.
- 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 to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems/internet will be posted in all rooms with student ICT access and displayed on log-on screens of both students and staff.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – parents / carers

The school will seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parent Voice Forum.
- Reference to external e-safety websites through a page on the school website

- Information sessions provided by the schools and external agencies such as The Police and SWGfL

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 meets the E-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority e-Safety Policy and guidance.

Servers, wireless systems and cabling must be securely located and physical access restricted where possible.

All users will have clearly defined access rights to school ICT systems through group policy. Users can be made aware of their own group policy access rights at any time by contacting the ICT department, although any requested changes to these access rights is solely at the discretion of the ICT manager. Any changes must comply with this e-safety policy and the AUP of the requesting individual.

All users will be provided with a username and password by the ICT Manager who will keep an up to date record of users and their usernames.

The “master/administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the relevant Headteacher or other nominated school leader and kept in a secure place (e.g. 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 the South West Grid for Learning.

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 relevant Headteacher (or other nominated senior leader).

Any filtering issues should be reported immediately to SWGfL.

Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Network manager and SLT.

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.

An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system. All temporary staff must sign the staff AUP and be made aware of this e-safety policy

An agreed policy is in place through the AUPs regarding the downloading of executable files by users

An agreed policy is in place through the AUPs regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on laptops and other portable devices that may be used out of school

An agreed policy is in place through the AUPs regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations / portable devices.

The school infrastructure and individual workstations are protected by up to date virus software.(Sophos).

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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism,

drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager temporarily remove those sites from the filtered list for the period of study. Any request to do so must be recorded by the requesting member of staff. A request from can be found in the ICT office.

- Students / pupils 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 / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, 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.

Careful consideration should be given as to how activities involving the taking of images are organised and undertaken. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them. Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings.

It is not appropriate for adults to take photographs of children for their personal use.

Digital/Video Images Policy

1. Members of staff and volunteers will only use school equipment to make digital/video images of students or adults associated with the school. No image will be made using personal equipment.
2. Any image made will be destroyed when no longer needed for the activity for which it has been produced.
3. All parents and carers will be asked on an annual basis to indicate if they do not wish images of their child to be used in published materials.
4. Any images of students which are published will be used in a manner which does not allow identification by name. Exceptions to this guideline will only be made when publication of an image is linked to a particular achievement of a student or group of students and specific permission has been obtained from the family or families concerned.
5. Images/videos recorded using the relevant school's CCTV system are not covered by this policy but are subject to a separate policy to which reference should be made.

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, 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 be checked using an approved virus checker before any data is stored on it.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed with permission	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	*				*			
Use of mobile phones in lessons		*					*	
Use of mobile phones in social time	*				*			
Taking photos with school equipment	*					*		

Taking photos on mobile phones				*			*	
Use of mobile devices eg Ipads, Ipods.	*					*		
Use of personal email addresses in school, or on school network			*					*
Use of school email for personal emails				*				*
Contributing to social networks for educational purposes e.g. wallwisher, Twitter, YouTube	*				*			
Use of social networking sites	*			*				*
Use of blogs		*				*		

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. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, 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, Twitter, Facebook, YouTube 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.
- All students will be provided with individual school email addresses for educational use.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Twitter

Twitter is used solely as a method of publicising information. If you follow us you can expect between 5-10 Tweets a week covering subjects such as:

Coverage of significant events in school

Celebration of successes

Emergency information (For example, school closure due to snow).

At no point will either school follow anyone. It is still possible, however, to view profiles of followers of the school, but the school will not. There is no expectation on students and parents to follow the school as this requires a personal Twitter account. Students can, however, keep updated with recent Tweets via the school website or by entering www.twitter.com into a search engine.

At no point should staff follow or accept a follow from students.

@Replies and direct messages

The school believes in collaboration, however, we do not respond to direct messages via Twitter. We see Twitter as a one way form of communication. If you need to contact the school then please use the normal channels of communication.

YouTube

The school YouTube Channel is for sharing important video that specific subjects use, revision materials and significant events. Students and parents are encouraged to subscribe (no obligation). The school will not subscribe to any channels. See Digital/Video images policy for guidance (Page 14).

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
	child sexual abuse images				*

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:	**promotion or conduct of illegal acts, eg 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 UK				*
	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				*
Using school systems to run a private business					*
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or 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)				*
Creating or propagating computer viruses or other harmful files				*
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			*	
File sharing (using p2p networks such as U Torrent)				*
Use of social networking sites for educational purposes		*		

Use of social networking sites for private purposes				*
Use of video broadcasting eg Youtube		*		

Responding to incidents of misuse

It is hoped that all members of the Trust 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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Flow charts in appendix A should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Equally the school will follow the policies laid out in the safeguarding documentation and will inform necessary member of staff immediately to ensure the safeguarding of our young people.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the Trust will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils – Guidance on Actions and Sanctions

Incidents:	Refer to class teacher /	Refer to Head of Department / Head of	Refer to SLT	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	*	*	*	*	*	*	*
Unauthorised use of non-educational sites during lessons	*	*			*	*	*
Unauthorised use of mobile phone / digital camera / other handheld device	*	*			*	*	

Unauthorised use of social networking / instant messaging / personal email	*	*	*		*	*	*
Unauthorised downloading or uploading of files	*	*			*	*	*
Allowing others to access school network by sharing username and passwords	*	*			*	*	*
Attempting to access or accessing the school network, using another student's / pupil's account	*	*			*	*	*
Attempting to access or accessing the school network, using the account of a member of staff	*	*	*		*	*	*
Corrupting or destroying the data of other users	*	*			*	*	*
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	*	*	*	*	*	*	*

Continued infringements of the above, following previous warnings or sanctions	*	*	*	*	*	*	*
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	*	*	*		*	*	*
Using proxy sites or other means to subvert the school's filtering system	*	*	*		*	*	*
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*			*	*	
Deliberately accessing or trying to access offensive or pornographic material	*	*	*	*	*	*	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	*	*	*	*	*	*	

Staff Guidance on Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher	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).		*	*	*			*	*

Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	*							
Unauthorised downloading or uploading of files	*				*			
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	*		*		*			
Careless use of personal data eg holding or transferring data in an insecure manner	*							

Deliberate actions to breach data protection or network security rules	*	*	*		*	*	*	*
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	*	*	*					
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	*	*	*					
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	*	*						

Actions which could compromise the staff member's professional standing	*	*	*					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	*	*	*			*	*	*
Using proxy sites or other means to subvert the school's filtering system	*	*	*					
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*	*		*			
Deliberately accessing or trying to access offensive or pornographic material	*	*	*		*	*	*	*

Breaching copyright or licensing regulations	*							
Continued infringements of the above, following previous warnings or sanctions	*	*	*		*	*	*	*