BRANNEL SCHOOL

E-Safety Policy

Written by: Mr P Carpenter

Approved by Governors: Autumn 2015

Next Review: Autumn 2017

Background / 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.

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. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

It is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies etc.).

Schedule for Monitoring / Review

- The implementation of this e-safety policy will be monitored by the: E-Safety Coordinator and the Senior Leadership Team
- The E-Safety Policy has been agreed by the Senior Leadership Team and approved by Governors
- The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: Autumn 2014
- Should serious e-safety incidents take place, the following external persons / agencies should be informed: CEOP, LA, Police

Scope of the Policy

- This policy applies to all members of the school community 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 pupils 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 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.

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach.

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

- A planned e-safety programme will be provided as part of ICT and reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

Education – parents / carers

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

- Parents evenings
- School website

Education & Training – 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.

Training – Governors

- All Governors should take part in e-safety training/awareness sessions.

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 Acceptable Usage Policy
- The school has provided enhanced user-level filtering through the use of the Smoothwall filtering programme.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Headteacher.
- Remote management tools are used by staff to control workstations and view users activity

Reporting an E-Safety Incident

- Should an E-Safety issue arise then the current incident form should be used as normal with a tick placed in the E-Safety box.
- The completed form should be passed to the E safety Co-ordinator who will decide in conjunction with CPO and HoH the next steps.

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, Internet sites should be pre checked prior to pupil access.
- Access to You Tube will be granted to staff only and it is staff responsibility to check the suitability of material.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.

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**.

Students / pupils must not take, use, share, publish or distribute images of others without their permission

Digital Communications

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.
- 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. Please see the school's Social Networking Policy for greater guidance on the use of Social networking sites.

See Appendix 1 for further guidance on acceptable use.

Unsuitable / inappropriate activities

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.

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.

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

See Appendix 2 and Appendix 3 for activities which the school deems unsuitable and the actions which should be taken should you find/suspect unacceptable material.

Appendix 1 - 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 at certain times	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 on mobile phones or other camera devices				✓				✓
Use of hand held devices eg PDAs, PSPs	✓				✓			
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails		✓			✓			
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs	✓						✓	

Appendix 2 - Unsuitable / inappropriate activities

The school believes that the following activities would be inappropriate in a school context and that users, as defined below, should not engage in these 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	Unacceptable and illegal
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 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 (e.g. 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					✓	
File sharing					✓	
Use of social networking sites (Please see Brannel School Social Networking Policy)					✓	
Use of video broadcasting e.g. Youtube			✓			

Appendix 3 - Responding to 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

The SWGfL flow chart – below and should be consulted and actions followed in line with the flow chart.