BUSBRIDGE CE (Aided) JUNIOR SCHOOL

E-Safety Policy

This policy was updated and approved by the Governing Body in the spring term 2020
It will be reviewed in the spring term 2022

Version 21.09.2021

Writing and reviewing the e-safety policy

This e-safety Policy is part of our Safeguarding procedures and relates to other policies including those for ICT, anti-bullying and child protection.

Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.

Teaching and learning

Why internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school internet access is provided by Surrey County Council through a regional broadband contract, which includes filtering appropriate to the age of pupils.
- 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 safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate internet content

- The school will seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant internet content. For pupils whose parents lack economic or cultural educational resources, the school should

build digital skills and resilience acknowledging the lack of experience and internet at home.

- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

Managing internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive 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.
- Staff to pupil electronic communication must only take place within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address,

email and telephone number. Staff or pupils' personal information will not be published.

- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in tweets, blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- When permission has NOT been granted for photos to be used they will not be displayed on the website/ VLE and staff should check with DSL / Deputy DSL on their use in classroom displays.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing on the school learning platform

➢ Pupils must not place personal photos on any social network space provided in the school learning platform.

Managing filtering

➢ The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.

➢ If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.

➢ Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

➢ A log of any incidents may be useful to identify patterns and behaviours of the Pupils.

Managing emerging technologies

➢ Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

➢ Mobile phones belonging to children must be handed into the school office at the start of the day and collected at the end of the day.

- Staff mobile phones will not be used in lesson time.
- Staff will not take photos of pupils on their phones; please use the school cameras.
- On rare occasions it may be appropriate to take a photo of pupils using a teacher's personal device (e.g. at an out-of-school event), but permission must be sort from SLT beforehand and the photos deleted asap.

➢ Staff will use a school phone where contact with parents is required.
The school phone will be taken on all school trips

➢ The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

➢ Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising internet access

➢ All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. This will be requested annually.

➢ The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

➢ Parents will be asked to sign and return a consent form when their child joins the school.

- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access. The school will monitor ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

- Internet content will usually be pre-selected and children will be directed to saved images/video etc using the professional judgement of staff, thus avoiding the chance of pop-ups and adverts etc appearing that are inappropriate. Child safe search engines should be used to develop research skills safely.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the school complaints procedure.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with the school e-safety policy.

Communications Policy

Introducing the e-safety policy to pupils

- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils. This should be addressed each year as students become more mature and the nature of newer risks can be identified.

Staff and the e-safety policy

- All staff will be given the school e-safety Policy and its importance explained.
- Upon appointment all staff will sign to acknowledge that they have read and understood the e-safety policy and agree to work within the agreed guidelines.

- Staff will annually re-acquaint themselves with this document and sign the staff list to confirm that they still abide by the content of the policy.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior leadership and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the school e-safety Policy in newsletters and on the school web site.
- The school will ask all new parents to sign the parent /pupil Acceptable Use Agreement when they register their child with the school.
- Parents should be encouraged, where possible to interact with their children on the internet as well as provide other opportunities for learning and recreation.

Changes to this policy to aid effective teaching, learning and well-being during the Covid-19 school closure and future Home Learning (April 2020)

The changes below have been approved by the SLT.

(i) Named LSAs will be authorised to save children's pictures (which may contain images of the child) on their home computers when working on projects for the school Virtual Learning Environment. They may use their home PC as a conduit to download work from one area of the VLE and then upload onto another area of the VLE. They will delete images from their home device once this process has been completed.

(ii) Any images being shared on the VLE are done so with parental permission. Parents give permission by the fact that they have uploaded the pictures. Children are asked to check with their parents before uploading images and images are screened for suitability before uploaded for whole school viewing. Children need to be fully dressed and engaged in appropriate activity with appropriate background settings in order for a photo to be deemed suitable for the VLE. Once a photo is uploaded onto the VLE, it is posted in an area that can be viewed by peers with the main purpose being for children to share their home learning and lockdown activities with peers.

(iii) Staff will communicate with parents and children using the VLE, e mail or if required on the telephone. No staff member will communicate with a child using a child's own e mail address. On occasion, a teacher might communicate with a child via the child's parent email, however our preferred way for staff to communicate with children is through the VLE messaging service. The VLE messaging system is set up on a secure platform and messages can be monitored by the administrators. The head teacher and Deputy Head teacher, who are also the DSL and Deputy DSL, are administrators and monitor the messaging system. There is a 'swear filter' on the system and the administrators are alerted if a swear word is used. Children can also report any abusive or inappropriate messages. Staff are able to message children via the VLE and during school

closure this has been deemed appropriate in order for children to share any comments or queries about their work, to speak to a member of staff if they are worried about something and for staff to support children with work. All messaging is carried out in line with the schools Safeguarding Policy and staff will report anything that they are concerned about to the school DSLs.

~ / ~