BUSBRIDGE CE (Aided) JUNIOR SCHOOL

E-Safety Policy

This policy was updated and approved by the Governing Body in the autumn term 2024
It will be reviewed in the autumn term 2026

Version 23.09.2025

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.

We are aware that E-Safety out of school is a huge issue. We will always address out-of-school issues involving our pupils when we are made aware of them.

Our E-Safety Lead is Mr David Evans, devans@busbridge-junior.surrey.sch.uk .

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 safe and effective 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 managed by our out-sourced IT support (JSPC) they provide a service 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. E.g. plagiarism.
- 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 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 are managed by JSPC and reviewed by the school in conjunction with their recommendations.

Online communication

- Pupils and staff may only school e-mail accounts for school business.
- Pupils must immediately tell a teacher if they receive an offensive e-mail or message when using their school accounts.
- Pupils must not reveal personal details of themselves or others in school online communication, or arrange to meet anyone online, or in person.
- Staff to pupil electronic communication must only take place within the school approved systems and will be monitored.
- Caution should be used when viewing incoming e-mail and should be treated as potentially suspicious and attachments not opened unless the author is known.
- In our school children do not use email to contact external bodies.
- The forwarding of chain letters/emails is not permitted.

Published content and the school website

- The contact details on the website 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 seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- When permission has NOT been granted for photos to be used they will not be displayed on the website/ VLE.
- Parents should be clearly informed of the school policy on image taking and publishing of the images

Managing filtering

- The school will work in partnership with JSPC/Virtual ICT 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 Lead (Mr David Evans, devans@busbridge-junior.surrey.sch.uk) e.g. the big red button on the children's PC desktops
- 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 is kept which can help to identify patterns and behaviours of pupils.

Managing emerging technologies

- From September 25 we are a Smartphone-Free school for children. This means that children are not allowed to bring a Smartphone with internet access onto the school site, either during the school day or at school events. Children are allowed to bring in a brick-phone with no internet access.
- Appropriate phones belonging to children (see above) must be handed into the class teacher at the start of the day and collected at the end of the day. Pupils must not use phones on the school site or off school site at school events.
- Staff mobile phones must not be used on or off school site when children are present, however staff are encouraged to take mobile phones outside during a fire evacuation if possible. On occasions SLT provide permission for specific usage e.g. on coaches on school trips to provide location information
- During a signalled school Lock Down staff are instructed to use their mobile phones for communications with the school leadership team.
- Staff and other adults in school 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.
- The appropriate use of AI and Learning Platforms (VLE) will be discussed as the technology advances.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff are encouraged to take their personal mobile phones on school trips to facilitate effective communications with the school office /SLT.
- Staff will use a school phone (landline) where contact with parents is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school also has a Data Protection policy, which can be viewed on the school website.

Policy Decisions

Authorising internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. Reading of this will be requested annually.
- Parents will be asked to sign and return an 'Acceptable Use' agreement 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 JSPC 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, by the DSL team, in accordance with school child protection procedures.
- Parents are 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 guidelines will be shared with children, and displays and posters will be used to remind children of these.
- Pupils will be informed that network and internet use will be monitored.
- At the start of each school year all pupils and their parents will be issued with, and asked to agree with, our Pupil Internet Usage Agreement document. The content of this agreement will be reinforced in class throughout the school year.
- 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. (See Appendix 1)

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.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the school E-Safety Policy in newsletters and on the school website.
- The school will ask all new parents to facilitate their child signing the pupil 'Acceptable Use' Agreement when they register their child with the school.
- At the start of each school year parents will be issued with, and asked to agree with, our Pupil Internet Usage Agreement document (Appendix Three).
- Parents should be encouraged, to engage with and monitor their children's use of the internet as well as provide other opportunities for learning and recreation.
- We will support parents with E-Safety at home by providing guidelines in the Curriculum Information Evenings and on the school website/in-school communications.
- Appendix 2 outlines our policy and procedures should a period of Home Learning be required by the whole school or a specific cohort.

Appendix 1 : Coverage of E-Safety in our school curriculum

Appendix Two : Policy and Procedures re Home Learning (September 2024)

Appendix Three : Pupil Internet Usage Agreement

Appendix 1 : <u>Coverage of E-Safety in our school curriculum</u>

- We are fully aware that our children are most at risk when accessing and using the internet out of school time. We talk about and deal with out-of-school issues when we are made aware of them in a bid to keep our pupils safe.
- We provide opportunities within the Computing and PSHE curriculum areas to teach about E-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is carried out as part of the curriculum, and informally when issues/opportunities arise.
- As part of our school curriculum, pupils are taught about consent, copyright and respecting other people's information, images, etc. This is done through discussion, modelling, and teaching and learning activities.
- Pupils are aware of the impact of online bullying. This is taught through the PSHE curriculum as well as wider whole school activities such as assemblies and themed weeks. Pupils are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying, gaming).
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know.

Our work in this area reflects the KCSIE (2025) guidance on Online Safety:

134. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

135. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

***content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.*

***contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.*

***conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying,*

***commerce**: risks such as in-game 'loot boxes', online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).*

136. Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

Through our planned curriculum and incident-led/child-led unplanned provision we cover the 4Cs of Online Safety, as outlined above in in KCSIE (2025).

	Topic / Themes covered	**Example of curriculum content**
Year 3	Staying safe online Who to tell if… Passwords Safe searching	Children develop strategies for staying safe when searching for content whilst using the Internet.
Year 4	Staying safe online Safe searching Who to tell if… How to block and report Adverts and clicking on unknown links / adverts Don't meet up	Evaluate online content to decide how honest, accurate, or reliable it is, and understand the consequences of false information. Identify a range of ways to report concerns about content and contact
Year 5	Staying safe online Who to tell if… Blogs staying safe, what to publish, who to tell if… Don't meet up Inappropriate messaging Cyberbullying Digital footprint Sharing rules	Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour.
Year 6	Staying safe online Who to tell if… Gaming and chat rooms in games Don't meet up Inappropriate messaging Cyberbullying Digital footprint Sharing rules Risks and pitfalls of social media such as WhatsApp, Tiktok (photos, messaging, permissions, consent, ownership, 'not really deleted', screenshots).	Identify a range of ways to report concerns about content and contact Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

Appendix Two : Policy and Procedures re Home Learning (September 2024)

In the rare event of children needing to access Home Learning the following will apply.
The form and frequency of teacher-class contact will be agreed on a case-by case basis.

(i) Named members of staff will be authorised to save children's pictures (which may contain images of the child) on their home computers (unless they have a school-issue laptop) 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. The images are uploaded into a secure area so that staff can screen them for suitability before bring 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 home activities with peers.

(iii) Staff will communicate with parents and children using the VLE, email or if required on the telephone. No staff member will communicate with a child using a child's own email 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.

(iv) 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 an 'inappropriate language filter' on the system and the administrators are alerted if such a word is used. Children can also report any abusive or inappropriate messages by using the Report button. Staff are able to message children via the VLE. During school closure this is 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 Child Protection and Safeguarding polices. Staff will report anything that they are concerned about to the school DSLs.

~ / ~