



Brabourne CE Primary School

Online / e-Safety Policy – October 2019

This policy has been prepared with the Christian Value of responsibility foremost – this is a core value of the school and all members of the school community aspire to live by it daily. Governors and staff are responsible for the safety of pupils – and that includes teaching them how to be responsible for themselves in all aspects of their lives.

“Responsibility means that we are all safe and that we look after ourselves, our school and each other”-Year 5 pupil.

1. Why is Internet use important?

- a) The Internet is a part of everyday life for education, business and social interaction.
- b) The school has a duty to provide students with quality Internet access as part of their learning experience.
- c) The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management functions.

2. How does Internet use benefit education?

Benefits of using the Internet in education include:

- a) access to worldwide educational resources;
- b) access to learning wherever and whenever convenient.
- c) educational and cultural exchanges between pupils worldwide;
- d) educational materials and effective curriculum practice;
- e) professional development for staff through access to national developments,
- f) collaboration across networks of schools, support services and professional associations;
- g) improved access to technical support including remote management of networks and automatic system updates;
- h) exchange of curriculum and administration data with KCC and DfE;

3. How can Internet use enhance learning?

- a) The school’s Internet access will be designed to enhance and extend education.
- b) Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- c) Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- d) Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils’ age and ability.
- e) Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- f) The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

4. How will pupils learn how to evaluate Internet content?

- a) Pupils will use age-appropriate tools to research Internet content.
- b) Older pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

5. How will information systems security be maintained?

- a) The security of the school information systems and users will be reviewed regularly.
- b) Virus protection will be updated regularly.
- c) Staff are provided with encrypted memory sticks or 'hosting' cloud based storage.
- d) Files held on the school's network will be regularly checked.
- e) User logins and passwords must be enforced where there is confidential information or to restrict access to security settings; however, to allow easier use of IT by young pupils, there may not be such strict enforcement of routine curriculum work. Staff will be promoted to change their passwords periodically.

6. How will email be managed?

- a) Pupils may only send or receive email as authorised by the school and solely for educational purposes and under staff supervision.
- b) Staff may only access emails during break times when they are not supervising pupils and it must not interfere with their duties.

7. How will school website be managed?

- a) The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- b) The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- c) Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- d) Parents/carers are asked when their child begins school whether they give permission for the school to use their child's image on the website and on the school's social media account. They also have the right to ask the school to withdraw any image or work of their child from the school website at any time.

8. How will social networking, social media be managed?

- a) The school's filtering system will control access to social media and social networking sites.
- b) Staff wishing to use Social Media tools with students as part of the curriculum will risk-assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.

9. How will filtering be managed?

- a) The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- b) The school will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed.
- c) If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

- d) A weekly report will be generated by Lightspeed and viewed by the Headteacher of pupil and staff searches.

10. How will risks be assessed?

- a) The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- b) The school will audit IT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- c) Methods to identify, assess and minimise risks will be reviewed regularly.

11. How will the school respond to any incidents of concern?

- a) All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyber-bullying, illegal content etc).
- b) The e-Safety Coordinator (Mr Stapley) will record all reported incidents and actions taken in the school e-Safety File and in any other relevant areas e.g. Child protection log.
- c) The Designated Child Protection Coordinator (Mr Stapley) or in his absence (Mr Taylor), will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- d) The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- e) The school will inform parents/carers of any serious incidents of concerns as appropriate.
- f) Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children’s Safeguard Team or e-Safety officer and escalate the concern to the Police.
- g) If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children’s Officer or the County e-Safety Officer.

12. How will e–Safety complaints be handled?

- a) Complaints about Internet misuse will be dealt with under the School’s complaints procedure.
- b) Any complaint about staff misuse will be referred to the head teacher.
- c) All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- d) All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

13. How will Cyber-bullying be managed?

- a) Cyber-bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s policy on anti-bullying and behaviour.
- b) Any reports of cyber-bullying will be investigated by the e-safety coordinator and a record kept of the investigation.

- c) The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

14. How will mobile phones and personal devices be managed?

- a) Pupils should not have mobile phones during school hours – if they are brought in they should be handed into the office for safe keeping until the end of the day.
- b) Staff mobile phones and personal devices must not be used during lesson time unless specifically in support of lessons.

15. How will the policy be introduced to pupils and staff?

- a) All users will be informed that network and Internet use will be monitored.
- b) At the start of each year, pupils will be reminded of safe internet use; they will also be reminded in computer lessons throughout the year and take part in events such as Safer Internet Day to raise the awareness and importance of safe and responsible conduct.
- c) Training on e-safety will be provided for staff.
- d) Staff will be made aware that their online conduct out of school could have an impact on their role and reputation within the school. Disciplinary action could be taken if they are found to bring the profession or school into disrepute, or if something is felt to have undermined confidence in their professional abilities.

16. How will this policy be monitored?

- a) This policy will be monitored by the e-safety coordinator and the Governor responsible for safeguards.
- b) It will be reviewed every two years by the staff and Governors for their approval.