Castle View Primary School

Keswick Road, Lancaster, LA1 3LE
Tel. 01524 67880
Headteacher: Miss Claire Bright

ONLINE SAFETYPOLICY

Date updated by staff	
Date approved by Governors	
Review Date	

Online Safety Policy

1. Online Safety Policy

The **Online Safety Policy** is part of the **school's Computing Policy** and relates to other policies including those for safeguarding, behaviour, for personal, social and health education (PSHE) and Citizenship. This policy also refers to the Teaching and Learning policy,which states that "in order to create a diverse, child-centred learning environment that engages, inspires motivates and appropriately challenges each individual, we will: extend experience within modern technology including our Home Learning area."

Reference to staying safe whilst using modern technologies is made in the scheme of work for PSHE and Citizenship.
Our Online Safety Policy has been written by the school, building on the LGfL policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

2. Why is internet use important?

- 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 information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

3. How does the internet benefit education?

Benefits of using the internet in education include:

- access to world-wide educational resources;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;

- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA, DfE and other organisations;
- mentoring of pupils and providing peer support for them and teachers.

4. How will internet use enhance learning?

- The school internet access is designed expressly for pupil and staff use and will include 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.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity (see learning policy – learning and teaching strategies).
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

5. How will pupils learn to evaluate internet content?

- As part of our computing curriculum, children will learn which sites are most appropriate and how to use the internet with appropriate behaviours.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing subject leader who will take appropriate action.
- The school should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge when internet sources have been used for information, with the reference 'information from the internet' quoted on work.

6. How will e-mail be managed?

- Pupils 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 details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Whole-class or group e-mail addresses should be used at EYFS and Key Stage 1. Where individual emails are used at Key Stage 2, these will be monitored by the class teacher and/or Computing subject leader and school computing technician.

7. How should website content be managed?

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be carefully selected.
- Pupils' full names will not be used anywhere 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.
- Any images shared with external providers will be carefully reviewed and selected and will only show pupils with published photograph consent.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's, DfE's and local authority's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

8. Can Chat be made safe?

- Pupils will only be allowed access to school specific chat rooms or forums and all use will be supervised and monitored.

9. How can emerging internet applications be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- School staff will advise the Computing Subject leader if they feel a particular program or app used in school is or has become unsuitable for use in part or entirety. Use of the program or app will be reviewed and appropriate steps taken.

10. How will internet access be authorised?

- The school will keep a record of all staff and pupil IT accounts. The record will be kept up-to-date, for instance a member of staff or child may leave or access may be withdrawn.
- All children will be supervised when using the internet and will receive, as part of the school's Computing scheme of work, an Online Safety curriculum to guide on safe use.
- Parents will be asked to give consent for children to use the internet.

11. How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LCC can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- The Headteacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

12. How will filtering be managed?

- Filtering may be performed by a combination of the ISP, by the LA and at school-level
- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Staff and pupils will only use the search engines as recommended by school.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing subject leader who will take appropriate action.
- It will be the responsibility of all to ensure safe use of the internet and filtering systems must not be relied on to be 100% accurate.

13. How will the policy be introduced to pupils?

- Rules for Internet access will be posted in all rooms where computers are used.
- Pupils will be informed that internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.
- A module on responsible internet use (at school and at home) will be included in the whole school Computing scheme of work.

14. How will staff be consulted?

- All adults in school will be signposted towards the school's policies including Online Safety and responsible internet use as part of their induction.
- All adults should be aware that IT use can be monitored and traced to the individual user. Discretion and professional conduct are essential.

15. How will complaints regarding internet use be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaint's procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions available include:
  - interview by Senior Leadership Team;
  - informing parents or carers;
  - removal of internet or computer access for a period.

16. Photographs and videos

- Photographs and/or videos of pupils may be taken with school mobile digital media devices and used in line with school policies and with parental consent.
- Adults and children in school may not use personal mobile digital media devices (e.g. mobile phones) to take photographs or videos of children.
- The only exception to this is for families attending public events such as Sports Day or Nativity Plays. In these circumstances a member of staff will make an announcement that families may use their own devices to take photographs and videos, but these should focus on their own child, and should not be published on the internet or shared electronically in any way.
- Cross reference to Child Protection Policy section 13.

17. Mobile Phones

- Mobile phones may not be used in front of pupils. They may only be used in the school office and staffroom area of school, where pupils are not present.
- There are school mobile phones for some of the staff that can be used in front of the children. There are to be no cameras on these phones to maintain safeguarding.
- Cross reference to Child Protection Policy section 13.

18. Data Handling

- The School Business Manager is responsible for electronic transmission and receipt of pupil and staff data by secure means – including use of encrypted email and School2School.
- All adults in school must ensure that sensitive data is only transmitted by secure methods including encrypted email, data storage or website.
- All adults in school must ensure that sensitive data is only stored on the school server or encrypted data storage. This data must only be accessed through password request

- All adults in school will be made aware of the necessity for handling all data in line with the Data Protection Act 1998.

19. Links to other documents

- RCPS Safeguarding and Child Protection Policy.
- DfE Guidance for Safer Working Practice for Adults who work with CYP in Education Setting.
- LCC guidance on the use of social networking sites and other forms of social media.
- RCPS Responsible Internet Use – staff and pupil guidelines.
- RCPS Computing policy and scheme of work.
- The Data Protection Act 1998.
- RCPS Security Policy.
- RCPS PSHE & Citizenship policy and scheme of work.
- Rules for Responsible Use of Electronic Communications and Storage for Staff
- Rules for Responsible Use of Electronic Communications and Storage for Staff

Policy to be reviewed every year

Date of Reviewed Policy: June 2016 reviewed Dec 2016, Reviewed April 2019

Review Date: April 2021

Person responsible: C Bright