Lockington CE VC Primary School

E-Safety Policy

Date Policy Formally Agreed By Governors	March 2023
Date Policy Becomes Effective	November 2022 (working draft)
Review Date	March 2025
Person Responsible for Implementation and Monitoring	Computing Subject Leader

1. Introduction

This policy outlines the organisation and management of E-Safety at Lockington CE VC Primary School.

It is written within the context of our school's mission statement:

Our school is committed to working together to develop lively, enquiring minds and to promoting outstanding standards of achievement in a happy, safe and caring environment, based on Christian values, which encourage all to show respect, acceptance and understanding of others.

It has also been written in the context of our school's Christian vision, rooted in the teachings of Jesus:

'Let your light shine before others, that they may see your good works, and glorify your Father who is in heaven' (Matthew 5:16).

At Lockington Primary School we fully recognise, acknowledge and embrace the importance and benefits of a 'connected' world. The opportunities for learning created by providing access to such a world are limitless, and must therefore become part of day to day teaching and learning in school. Being part of the internet community, as well as providing the aforementioned opportunities, also opens up the possibilities of exposure to dangers which would otherwise not be present, for example: access to inappropriate materials; contact with potentially dangerous strangers; 'cyber' bullying and identity theft. It must therefore be the role of the school to ensure that such risks are minimized, and, more importantly, that children are provided with the knowledge, skills and attitude necessary to become positive, safe and healthy digital citizens.

2. Teaching and Learning

At Lockington Primary School we firmly believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings. The following aims demonstrate how this duty is fulfilled:

- We will provide a series of specific e-safety-related lessons in every year group/specific year groups as part of the computing curriculum / PSHE curriculum / other lessons.
- We will celebrate and promote e-safety through a several opportunities such as worship and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information

they use, and the need to respect and acknowledge ownership of digital materials.

- Staff will model safe and responsible behaviour in their own use of technology during lessons.

3. How Parents and Carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.
To achieve this we will:

- provide advice and guidance on e-safety should parents need any help;
- offer demonstrations and training to parents and carers;
- discuss e-safety issues at parents meetings;
- include useful links and advice on e-safety regularly in newsletters and on our school website;
- provide each parent with a copy of an e-safety booklet;
- include a section on e-safety in the School Prospectus and Home-School Agreement.

4. Managing IT systems and Access

The school will be responsible for ensuring that access to the IT systems is as safe and secure as possible. This will include making sure that:

- servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access;
- servers, workstations and other hardware and software will be kept updated as appropriate;
- virus protection is installed on all appropriate hardware, and will be kept active and up-to-date;
- the school will agree upon the appropriate level of access and supervision learners should receive;
- all users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using the school IT systems and that such activity will be monitored and checked;
- at EYFS / Key Stage 1 and Key Stage 2 pupils will access the use of their computer by using a log-on password and username. Internet access will be supervised AT ALL TIMES by a member of staff;
- members of staff will access the use of their computer using an individual log-on. They will abide by the school AUP at all times;
- any administrator or master passwords for the school IT systems should be kept secure and available to at least two members of staff, e.g. the headteacher and a member of technical support;
- the wireless network in school is encrypted to reduce the risk of unauthorised access to visitors and the local community;

- the school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. The school has a procedure to follow in the event of such occurrence;
- the school will regularly audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. We will regularly review our internet access provision, and review new methods to identify, assess and minimise risks.

5. Filtering Internet Access

Lockington Primary School uses a filtered internet service. The filtering is provided through East Riding of Yorkshire Council.

- If any user discovers a website with inappropriate content, this should be reported to a member of staff who will inform the Computing Leader, Safeguarding Leader and the Headteacher.
- If users discover a website with potentially illegal content, this should be reported immediately to the headteacher. The school will report this to appropriate agencies including the filtering provider and if necessary CEOP (www.thinkuknow.co.uk).
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

6. Learning Technologies in School

	Pupils	**Staff**
Personal mobile phones brought into school	No	Yes
Mobile phones used in lessons	No	No
Mobile phones used outside of lessons	No	Yes
Taking photographs or videos on personal equipment	No	No
Taking Photos or videos on school devices	Yes	Yes
Use of personal hand-held devices such as tablet computers or personal gaming consoles	No	No
Use of hand-held devices such as tablet computers or personal gaming consoles if provide by school.	Yes	Yes
Use of personal email addresses in school	No	No
Use of school email address for personal correspondence.	No	No
Use of online chat rooms	No	No

Use of instant message services.	No	Yes
Use of blogs, podcasts or social networking sites	Yes: controlled by filtering; always supervised	Yes: controlled by filtering
Use of video conferencing / online video meetings	supervised	Yes
Use of memory sticks	No	Yes - if encrypted and virus checked.

7. Using E-Mail

- Pupils are taught about e-mail and e-mail safety. Access to personal e-mails by children is not permitted in school. In the event that pupils are allocated approved e-mail accounts they are made aware that these are monitored and checked by the school.
- Staff must use their school e-mail address for communication between members of staff, others schools and agencies that they may come into contact with through the teaching role for content regarding the pupils and the school.
- Staff can use their own e-mail address but this must not be for communicating information or data about pupils.
- Pupils will be reminded when using e-mail about the need to send polite messages, about the dangers of revealing personal information, about the dangers of opening email from an unknown sender, or viewing/opening attachments.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

  Any inappropriate use of the school email system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

8. Using Images, Video and Sound

- We remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Digital images, video and sound will be created using equipment provided by the school, or equipment owned by staff who have signed the agreement in the staff Acceptable Use Policy, that images of children will not be kept on personally owned computer equipment.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in

accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.

- If pupils are involved, relevant parental permission will also be sought before resources are published online.

9. Using blogs, pictures, the school website and other ways for pupils to publish content on line.

Occasionally we use blogs, pictures and the school website to publish content online. This is done to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. It also provides meaningful and effective communication to parents and those with a link of interest to the life of Lockington Primary School. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Blogging and other forms of the publishing of online content by pupils will take place within the areas the school has provided for such material. This will be in the form of: the school website which is hosted by East Riding of Yorkshire Council.
- Pupils will model safe and responsible behaviour in their creation and publishing of online content within the school website. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them. Pupils will not use their name or the names of others when creating such resources.
- Staff and pupils will be expected and encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, social networking sites and other online publishing outside of school.

10. Mobile Phones

Pupils' personal mobile phones are not allowed in school. Staff are asked to carry and use their own mobile phones on school visits if needs be. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a parent and never to a pupil.

11. Using New Technologies

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-safety point of view when making such technologies available to learners.
- We will regularly amend the e-safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an e-safety risk.

12. Protecting Personal Data

- We ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the headteacher. Any data which is impractical to ensure is kept in school (e.g. reports) will be kept secure, by use of school laptops which are password protected.
- All staff are expected to store curriculum data including pupils performance scores and levels in secure and appropriate places. For example an encrypted memory stick, folders on staff school laptops and assessment files in classrooms.

13. School website and other on-line content published by the school

- The school website will not include the personal details, including e-mail addresses or full names, of staff or pupils.
- A generic contact e-mail address will be used for all enquiries received through the school website.
- All content included on the school website will be approved by the headteacher before publication.
- Staff and pupils should not post school-related content on any external website without seeking permission first.

14. Dealing with E-safety incidents

E-safety incident reports are available from the main office and in the Computing Subject Leader file. Once completed these must be submitted to the Headteacher (see Appendix 1).

15. **Responsibility for e-safety**

We believe that e-safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how the whole school community, teachers, staff, pupils, parents and carers, technical support staff and the Governing Body, will contribute.

Responsibilities specific to the whole school community

- Develop and promote an e-safety culture within the school community.
- Support the e-safety and safeguarding leaders in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to e-safety effectively.

- Receive and regularly review e-safety incident logs and be aware of the procedure to be followed should an e-safety incident occur in school.
- Take ultimate responsibility for the e-safety of the school community.
- Promote an awareness and commitment to e-safety throughout the school.
- Be the first point of contact in school on all e-safety matters.
- Maintain e-safety policies and procedures.
- Develop an understanding of current e-safety issues, guidance and appropriate legislation.
- Ensure that e-safety education is embedded across the curriculum.
- Ensure that e-safety is promoted to parents and carers.
- Liaise with the local authority, the local safeguarding children’s partnership and other relevant agencies as appropriate.
- Monitor and report on e-safety issues to the Computing and Safeguarding leads and Headteacher as appropriate.
- Ensure an e-safety incident log is kept up-to-date.

Responsibilities specific to teachers and support staff

- Read, understand and help promote the school’s e-safety policies and guidance.
- Develop and maintain an awareness of current e-safety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed e-safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an e-safety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities specific to the technical support staff

- Read, understand, contribute to and help promote the school’s e-safety policies and guidance.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school IT system.
- Report any e-safety-related issues that come to your attention to the headteacher, Computing and Safeguarding coordinators.
- Develop and maintain an awareness of current e-safety issues, legislation and guidance relevant to your work.
- Liaise with the local authority and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities specific to the pupils

- Help and support the school in creating e-safety policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies in school and at home.

- Take responsibility for your own and each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss e-safety issues with family, friends and teachers in an open and honest way.

Responsibilities specific to the Governing Body

- Read, understand, contribute to and help promote the school's e-safety policies and guidance.
- Develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- Develop an overview of how the school IT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the staff and pupils in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-safety activities.
- Ensure appropriate funding and resources are available for the school to implement their e-safety strategy.

16 Review

This e-safety policy was created by headteacher and the staff of Lockington CE VC Primary School. The person responsible is the Computing Subject Leader.

This policy will be reviewed every three years, or earlier as required.

Member of staff responsible: Computing Subject Leader/s

Date policy updated: November 2022

Date approved by full Governing Body: Spring 2023

Date for next review: November 2025

Signature (Head) Signature (Chair of Governors)

J Cattle

Julie Cattle (16.11.22) Kevin Beaumont (16.11.22.)