COPPICE VALLEY PRIMARY SCHOOL

COMPUTING & E-SAFETY PROCEDURE

Document History

Created / revised & approved by staff	March 2023
Viewed / modified / approved by	
Next review date	March 2025

COPPICE VALLEY PRIMARY SCHOOL

COMPUTING & E-SAFETY PROCEDURE

Overview
At Coppice Valley our Computing curriculum provides essential skills for life which enable learners to participate more readily in a rapidly changing world. Our curriculum retains the National Curriculum at its core. Wherever possible, we make real-world and cross-curricular connections i.e. photography & film making in topics.
Every child is able to access learning through quality first teaching and scaffolding lessons to meet pupils needs. Computing offers all pupils the opportunity to experience SMSC learning and FBV. Research expands pupils' knowledge of the world and its different cultures. E-safety and learning about online privacy generate ethical and moral discussions. As pupils progress, their vocabularies expand with technical words and phrases to give them the skills to express themselves.

Values Led-Learning
Brave: Children will challenge themselves by responding to opportunities to work both independently and in teams. They will make choices about how to develop and express their learning. They will be work on projects that stretch them and require them to show resilience and determination to succeed.
Curious: Computing is an essential life skill and offers the possibility to participate more readily in a rapidly changing world for the remainder of their education and adult life. This is at the forefront of all our computing lessons. Children will learn about the latest technologies and uses for computing. They will access and learn about the wider world through the internet.
Kind: We offer a safe environment for our children to access a diverse array of ideas and experiences from a wide range of people, communities and cultures. They will learn about diversity and equalities. Children will leave Coppice Valley knowing the importance of using the internet and social media with respect, tolerance and kindness.

Curriculum at each phase: E-Safety
Due to the ongoing risks that are posed to children on the internet, E-Safety is taught throughout the academic year. At each phase of education, our E-Safety teaching is planned with due regard to 'Teaching online safety in School" June 2019. We use Education for a Connected World and Project Evolve resources.
  - In EYFS we aim to ensure that children recognise the importance of technology and its purpose in places such as homes and schools. We provide a range of safe equipment to explore such as programmable toys, PCs, ipads and laptops. We explore what it does, and how to use it safely.
  - In KS1, we continue our E-safety learning. The purpose of this is to ensure that children understand the importance of staying safe online and to know where to go for help and support when they have concerns about content or contact on the internet.
  - In KS2, our E-safety curriculum continues. Building on prior knowledge from KS1, we ensure that children are accessing technology safely, respectfully and responsibly. Essential topics are covered in age and contextually appropriate detail: self-image and identity; online relationships; online reputation; online bullying; managing online information; health, well-being and lifestyle; privacy and security and copyright and ownership

Curriculum at each phase: Computing
In KS1 children will learn the following knowledge and skills:
  - Give simple instructions to everyday devices to make things happen.

- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions.
- Write and test simple programs.
- Make choices to control simple models or simulations.
- Use logical reasoning to predict the behaviour of simple programs.
- Complete simple tasks on a computer by following instructions.
- Show an awareness of information in different formats.
- Organise, store, manipulate and retrieve data in a range of digital formats.
- Discuss and share how and when they use ICT in everyday life.
- Recognise common uses of ICT beyond school.
- Understand rules around e-safety and know who to tell if something concerns them online.

In KS2 we look to establish a solid understanding of designing, writing and debugging programs that accomplish specific goals. We introduce variables and explore various forms of input and output. We provide a safe environment for children to select, use and combine a variety of software on a range of digital devices to accomplish given goals. Children will learn to:
- Use logical reasoning to explain how a simple algorithm works.
- Detect and correct errors in algorithms and programs (debug)
- With support, begin to produce algorithms by using logical and appropriate structures to organise data, and create precise and accurate sequences of instructions.
- Produce algorithms independently using logical and appropriate structures to organise and record data.
- Use sequence, selection and repetition in programs.
- Design and write programs that accomplish specific goals, working with variables for input and output.
- Use flowcharts and other diagrams to follow how the process or model works.
- Test programs using models and simulations.
- Use logical reason to solve problems and model situations and processes.
- Predict what will happen when variables and rules within a model are changed.
- Discuss opportunities for online communication and collaboration.
- Explain how email and online discussion areas are used for communication and collaboration.
- Create flowcharts and other diagrams to explain how a process or model works.
- Use software or search engines effectively.
- Check the plausibility and usefulness of information that they find.
- Understand the need for accuracy when searching for and selecting information.
- Create account of accuracy and potential bias when searching for and selecting information.
- Identify and select appropriate information using straightforward lines of enquiry.

- Use and combine a variety of software and internet services on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.
- Prepare and present information in a range of forms, using ICT safely and responsibly.
- Select, use and combine a variety of software, including internet services on a range of digital devices.
- Design and create/use a range or programs to accomplish given goals.
- Find and cite the web address for any information or resource found online.

Assessment
Pupils are assessed informally and formally by their teachers. These assessments are used to form the basis of the Computing section of the annual report to parents.

Equal Opportunities and Inclusion

- The school's ICT facilities are available for use by all pupils and staff. ICT is used to enhance each pupil's access to the curriculum. All pupils are able to make regular and varied use of the school's ICT facilities. ICT is used in a range of activities and in a variety of contexts.
- By its very nature Information Technology is accessible to children of a wide range of educational experience and attainment. For pupils with learning difficulties appropriate use of ICT can often enhance access to aspects of the curriculum. In co-operation with the SENCo the school will provide, wherever and whenever possible, appropriate software and hardware to enable such access.
- Pupils who show high levels of achievement in the use of ICT or for whom use of ICT can enhance high levels of achievement in other curriculum areas are given opportunities to extend their use of ICT.
- All pupils will have regular and equal access to a broad and balanced ICT experience across the whole curriculum.

Internet and Email

The school has broadband access to the internet. Every child is taught how to access the internet safely to find and display information. The school maintains a web site (www.coppicevalley.com) which is regularly updated with information on the children's work and links to other safe web sites. Teachers are responsible for updating their own year group areas. The school's procedure for the use of the Internet is set out in appendix 1.

Pupils will be protected from having access to undesirable materials by:

- close adult supervision;
- using only websites which have been checked for content by an adult;
- working off-line (sites will have been downloaded by adults, prior to use by pupils);
- working on-line, with an understanding that they will be held accountable for their own actions, as outlined in the 'School Internet Rules' document;
- knowing that if they see something which upsets them that they immediately switch off the monitor and tell an adult; and
- pupils will not have individual email addresses. An email address will be available for each class. An adult will always be present when email is received and opened.

Additional access for pupils who do not have a computer at home

The school is sensitive to those who have limited access to technology at home and attempts to increase access at school.

Resources

- Pupils will each have a personal directory on the computer network for the storage of temporary files. Computers will at all times be ready for use in the classrooms and shared areas. Hardware and software provision will be reviewed each year subject to the budget available. Where appropriate, training will be made available each year for all school staff according to need.

<div align="center">

Internet & e-safety Procedure

</div>

Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

Internet use will support, extend and enhance learning
• Pupils will be given clear objectives for internet use.
• Web content will be subject to age-appropriate filters.
• Internet use will be embedded in the curriculum.

Pupils will develop an understanding of the uses, importance and limitations of the internet
• Pupils will be taught how to effectively use the internet for research purposes.
• Pupils will be taught to evaluate information on the internet.
• Pupils will be taught how to report inappropriate web content.
• Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.
• Pupils will use the internet to enhance their learning experience.
• Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies. Pupils will use existing technologies safely
• Pupils will be taught about e-safety.
E-mail
• Pupils will tell a member of staff if they receive inappropriate e-mail communications.
Internet Access
• Staff will read and sign the Acceptable Use Policy before using any school ICT resource.
• Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.

Mobile Phones and other handheld technology
Pupils are only permitted to have mobile phones or other personal handheld technology in school with the permission of the Headteacher. When pupils are using mobile technology (their own or that provided by the school) they will be required to follow the school's safeguarding regulations for using technology. Such items can be confiscated by school staff if they have reason to think that

5

they are being used to compromise the wellbeing and safety of others (Education and Inspections Act 2006, Sections 90, 91 and 94).

School Website and Published Content.
• ICT systems security will be regularly reviewed with support from Red Kite IT services
• The school will work with Red Kite IT Services to ensure that appropriate filtering is in place.
• Pupils will report any inappropriate content accessed to an appropriate member of staff.
Communication of the e-safety policy to pupils
• E-safety rules will be posted around the school to remind the children of these and these will be discussed regularly in lessons.
• Pupils will be informed that internet and VLE use will be monitored.
• e-Safety will be included in the curriculum and regularly revisited

Communication of the e-safety policy to staff
• The Safeguarding Policy (including E-Safety & Safer Working Practices for Staff) will be given to all new members of staff as part of the staff induction.
• The Safeguarding Policy (including E-Safety & Safer Working Practices for Staff) will be signed by all staff and discussed with them at least annually.
• Staff will be informed that internet use will be monitored.

Communication of the e-safety policy to parents/carers
• The Safeguarding Policy (including E-Safety & Safer Working Practices for Staff) will be available from the school.
• The school website will include e-safety website information for parents to access.
• The school will communicate and publicise e-safety issues to parents through meetings in school and newsletters where relevant.

e-safety Complaints
• Instances of pupil internet misuse should be reported to the E-Safety co-ordinator (DSL).
• Staff will be trained so they are able to deal with e-Safety incidents. They must email E-safety incidents to the E-safety co-ordinator. The Safeguarding Policy, E-safety Section details the procedures to follow.
• Instances of staff internet misuse should be reported to, and will be dealt with by, the Headteacher. See the Safeguarding Policy for details of procedures to follow.

Whole-School Responsibilities for Internet Safety
Headteacher
• Responsible for e-safety issues within the school however day-to-day responsibility is delegated to the e-safety co-ordinator.
• Ensure that the e-safety co-ordinator is given appropriate time, support and authority to carry out their duties effectively.
• Ensure that developments at Local Authority and Trust level are communicated to the e-safety co-ordinator.
• Ensure that the Governing Body is informed of e-safety issues and policies.
• Ensure that appropriate funding is allocated to support e-safety activities throughout the school.

e-Safety co-ordinator
• Primary responsibility: establish and maintain a safe ICT learning environment (under the direction of Senior Management).

• Establish and maintain a school-wide e-safety programme.
• Respond to e-safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies, and maintain an incident log.
• Establish and maintain a staff professional development programme relating to e-Safety.
• Develop a parental awareness programme.
• Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

Governing Body
• Support the Headteacher and designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
• Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the Headteacher and/or designated e-safety co-ordinator (as part of the wider remit of the Governing Body with regards to school budgets).

Network Manager/Technical Support Staff
• Provide a technical infrastructure to support e-safety practices.
• Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.
• Ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.
• Develop an understanding of relevant legislation.
• Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the e-safety co-ordinator.
• Maintain a professional level of conduct in their personal use of technology, both within and outside school.
• Take responsibility for their professional development in this area.

Teaching and Support Staff
• Contribute to the development of e-safety policies.
• Adhere to Safer Working Practices advice in the Safeguarding Policy
• Take responsibility for the security of data.
• Develop an awareness of e-safety issues, and how they relate to pupils in their care.
• Model good practice in using new and emerging technologies.
• Include e-safety regularly in the curriculum.
• Deal with e-Safety issues they become aware of and know when and how to escalate incidents.
• Maintain a professional level of conduct in their personal use of technology, both within and outside school.
• Take responsibility for their professional development in this area.

Wider School Community
• This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet, Learning Platform or other technologies.
• Contribute to the development of e-safety policies.
• Adhere to acceptable use policies.
• Take responsibility for the security of data.
• Develop an awareness of e-safety issues, and how they relate to pupils in their care.
• Model good practice in using new and emerging technologies.
• Know when and how to escalate e-safety issues.

•   Maintain a professional level of conduct in their personal use of technology, both within and outside school.
•   Take responsibility for their professional development in this area.

Parents and Carers
•   Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
•   Discuss e-safety issues with their children, support the school in its e-safety approaches and reinforce appropriate behaviours at home.
•   Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
•   Model appropriate uses of new and emerging technologies.
•   Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.

Pupil E-safety Rules:-

Children will discuss the importance of e-safety in their classes regularly. Below is a suggested resource for class teachers to use with their classes, however teacher's need to assess how best to cover e-safety in their classes dependent on the age and ability of their children.

http://www.childnet.com/kia/primary/smartadventure/default.aspx

Be SMART, think before you click!

Safe
- I will ask for permission before using the internet
- I will use the internet sensibly by thinking before I do anything
- I will only send polite and friendly emails
- I will never give out any personal details

Meeting
- I will never arrange to meet strangers, even if I trust them

Accepting
- I will only open an email if it's from somebody I know

Reliable
- I will only click on links if I know where they will take me
- I will only open an email if it's from somebody you know
- I understand everything I see on the internet may not be reliable information and may need to re-check information I find on another website or look it up in a book.

Tell
- I will tell an adult if someone is making me feel uncomfortable
- I will tell an adult about anything that you see that worries me
- I will ask for help if I get lost when I am using the internet

Appendix 1

<table>
<tr><td colspan="2" style="background:#1a2744;color:white">ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS – KEY STAGE 1</td></tr>
<tr><td colspan="2">**Name of pupil:**</td></tr>
<tr><td colspan="2">

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

Ask a teacher or adult if I can do so before using them

Only use websites that a teacher or adult has told me or allowed me to use

Tell my teacher immediately if:

      o I click on a website by mistake

      o I receive messages from people I don't know

      o I find anything that may upset or harm me or my friends

Use school computers for school work only

I will be kind to others and not upset or be rude to them

Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly

Only use the username and password I have been given

Try my hardest to remember my username and password

Never share my password with anyone, including my friends.

Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer

Save my work on the school network

Check with my teacher before I print anything

Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.
</td></tr>
<tr><td>**Signed (pupil):**</td><td>**Date:**</td></tr>
</table>

Appendix 2

<table>
<tr><td colspan="2" style="background:#1a2744;color:white">ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS – KEY STAGE 2</td></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.
</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
</table>