Egerton Primary School

Computing and E-safety Policy

Approved by:	Neil McKinlay	**Date:**	29 September 2021
Last reviewed on:	September 2018		
Next review due by:	September 2024		

Our Aims

The use of computers and computer systems is an integral part of the National Curriculum and knowing how they work is a key life skill. In an increasingly digital world there now exists a wealth of software, tools and technologies that can be used to communicate, collaborate, express ideas and create digital content. At Egerton we recognise that pupils are entitled to a broad and balanced computing education with a structured, progressive, approach to the learning how computer systems work, alongside the skills necessary to become digitally literate and participate fully in the modern world.

At the heart of our school's ethos is the importance of global learning and creating local and global partnerships across the world; we recognize that digital technology places an essential part in achieving this goal. Through our use of the Lyfta global resource platform and our ongoing partnerships and video conferences with Egerton Primary in Kenya, digital technology is at the core of our pupils experiences as global citizens.

The school's aims are to:

- Provide a broad, balanced, challenging and enjoyable curriculum for all pupils.
- Develop all pupils' computational thinking, allowing them to problem solve in a digital context, which will benefit them throughout their lives and careers.
- Meet the requirements of the national curriculum programmes of study for computing at Key Stage 1 and 2.
- To respond to new developments in technology in terms of both the content of curriculum, as well as the pedagogy and resources used to deliver it.
- To equip pupils with the confidence and skills to use digital tools and technologies throughout their lives.
- To enhance and enrich learning in other areas of the curriculum using IT and computing.
- To develop the understanding of how to use computers and digital tools safely and responsibly (see: E-Safety and AUP).
- To utilize technological platforms, such as Lyfta, to provide pupils an unique, interactive and highly impact scheme of global learning.
- Continue to liaise with Egerton Primary in Kenya through video conferencing and online projects, building on the investment in our sister school's digital resources and internet access.

Early years:

It is important in the foundation stage to give children a broad, play-based experience of IT and computing in a range of contexts, including off-computer activities and outdoor play. Computing is not just about computers: children gain confidence, control and language skills through opportunities such as 'programming' each other using directional language to find toys/objects, creating artwork using digital drawing tools and controlling programmable toys. Outdoor exploration is an important aspect and using digital recording devices such as video recorders, cameras and microphones can support children in developing communication skills.

At Egerton, opportunities for computational learning and digital experiences are threaded throughout the EYFS curriculum, including resources from our *Purple Mash* software suite to ensure pupils are ready for their transition to KS1 and have a familiarity with the systems that provide the basis of their ongoing learning.

As per the national curriculum programme of study, by the end of key stage 1 pupils can:

- 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.
- use logical reasoning to predict and computing the behaviour of simple programs
- organise, store, manipulate and retrieve data in a range of digital formats.
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

As per the national curriculum programme of study, by the end of key stage 2 pupils can:

- design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.
- use sequence, selection, and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs.
- use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs.
- understand computer networks including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration.
- describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely.
- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Computing at Egerton

Curriculum:

As a staff, we are all aware that IT and computing skills should be developed throughout pupils' computing lessons, but also core and foundation subjects as well. IT and computing is used to support learning in other subjects as well as developing computing knowledge, skills and understanding, with special attention to embracing Egerton's unique theme-based curriculum. Our school provides pupils with opportunities to enrich and deepen learning using cross-curricular approaches, tying in closely with Egerton's use of Mantle of the Expert to make learning purposeful and rich with content.

Planning and Progression of Skills:

We use Purple Mash's scheme of planning across the school to provide confident coverage of the curriculum, a careful progression content and skills, as well as a smooth transition from each year group to the next. Alongside this framework, teachers plan, deliver and assess their teaching following the Progression of Skills in Computing document. These learning statements, built to cover the expectations and of the NC and beyond, also allows teachers to enhance and expand on the planning spine, all the while ensuring that all additional resources and learning is in line with the needs of their pupils. (See Appendices).

Inclusion & Assessment:

We believe that all children have the right to access IT and computing. In order to ensure that children with special educational needs achieve to the best of their ability, it is sometimes necessary to adapt the delivery of the computing curriculum for some pupils. This is done through careful planning and dialogue between the class teacher, subject leader and SENCo.

We teach IT and computing to all children, whatever their ability. Computing forms part of the national curriculum to provide a broad and balanced education for all children. Through the teaching of computing we provide opportunities that enable all pupils to make progress. We do this by setting suitable challenges and responding to each child's individual needs. Where appropriate, IT can is also used to support SEN children on a one-to-one basis where children receive additional support.

E-Safety at Egerton

Overview and Our Curriculum:

In recognition of the importance that digital platforms and communication will play in pupils' ongoing lives, the safe use of these technologies is at the heart of our Computing curriculum. This covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of digital technologies within our society as a whole. Both inside and outside the classroom we would expect our children to interact digitally with the world through a variety of devices, from computers and tablets, to mobile devices and smart watches. Pupils must prepared for the connected world ahead of them, including:

- Websites and Online Search engines
- Learning Platforms and Virtual Learning Environments, such as Lyfta, SeeSaw PurpleMash
- Email and Instant Messaging, such as WhatsApp
- Social Networking and Video Chats, including the chat functions within online games
- Video Streaming, both pre-recorded content often found on sites such as YouTube and live streaming which is increasingly popular on gaming-streaming platforms such as Switch
- Multiplayer Gaming, both with "real world" friends, online friends and strangers
- Music Streaming and Podcasting

All users need to be aware of the range of risks associated with the use of these Internet technologies, as well as the increasing prevalence of advertising - often not obvious - through these mediums.

As part of the *digital literacy* section of our programme of study, online safety is not only taught discretely through these computing sessions but additionally during PSHE lessons, whole school opportunities for learning such as assemblies or event days, as well as during other subjects where pupils might use technology, such as for email, blogging and online research.

As part of our Progression of Skills in Computing document, e-safety (within *digital literacy*) is carefully and deliberately mapped out into key learning goals across each year group, building progressively to ensure that every pupil leaves our school as a prepared and resilient digital citizen.(See Appendices).

Whole school approach:

All members of the school community have a responsibility for promoting and supporting safe

behaviours in their classrooms and follow school e-safety procedures. This includes vigilance when children are accessing the internet at school to ensure that they do not access inappropriate websites, as well as:

• safe use of e-mail
• safe use of the Internet
• safe use of the school network, equipment and data
• safe use of digital images and digital technologies, such as mobile phones and digital cameras
• monitoring publication of pupil information/photographs on the school website and our SeeSaw platform
• following the correct procedures in the event of misuse of technology by any member of the school community (see appendices)
• their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction. Supply Teachers and visitors must sign an acceptable use of ICT agreement before using technology equipment in school (see appendices for staff acceptable use agreement).

Children will have supervised access to internet resources within school, however:

• Staff must preview any recommended sites before use. (Particular care must be taken when using search engines with the children as these can return undesirable links.)
• Raw image searches are discouraged when working with pupils.
• If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.
• Our internet access is controlled through the Smoothwall web filtering service.
• Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
• If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported as soon as possible to a member of SLT and the computing lead.
• It is the responsibility of the school, by delegation to the technical support team, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

E-mail:

The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school, between schools or international (such as our work with Egerton in Kenya). We recognise that pupils need to understand how to style an email in relation to their age.

• Pupils are introduced to email as part of their Computing sessions using 2Email to simulate real conversations, monitored by the teacher.
• The school gives staff their own email account, to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
• Under no circumstances should staff contact pupils or parents using personal email addresses.
• Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

Publishing pupil's images and work:

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

• On the school web site, SeeSaw and school YouTube channel (where videos will be delisted with comments disabled).
• In display material that may be used in the school's communal areas.
• In display material that may be used in external areas, i.e. exhibition promoting the school.
• General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

Egerton Primary aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Responding to e-safety incidents/complaints:

As a school we will take all reasonable precautions to ensure the Egerton learning environment is e-safe. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies (such as our school iPads) and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.
The school cannot accept liability for material accessed, or any consequences of Internet access through the computers and iPads within school. Complaints relating to e-safety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Head teacher.

• All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
• Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Head teacher/ LEA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
• Pupils and parents will be informed of the complaints procedure.
• Parents and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying:

Cyberbullying can be defined as the use of electronic communication devices to bully a person. Electronic communication can include the use of computers, mobile phones, tablets and games consoles. Cyberbullying can take place through the use of emails, text messages, social networking sites such as Facebook and Twitter, chat rooms, interactive video games and in many other areas too. As technology advances, more potential avenues for cyberbullying open up. Examples of cyberbullying could include posting mean, offensive or embarrassing comments or photos on social networking websites, sending threatening or abusive emails, or creating fake online profiles to embarrass or belittle another person.

Cyberbullying in itself is not a crime and is not covered by a specific law in the UK. However, by committing an act of cyber bullying, a person may be committing a criminal offence under a number of different acts.

The whole school community has a duty to protect all its members and provide a safe, healthy environment. It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our digital literacy curriculum and within wider PSHE sessions.

Pupils should:
• understand how to use these technologies safely and know about the risks and consequences of misusing them.
• know what to do if they or someone they know are being cyber bullied.
• report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

In return, adults both in school and at home will:
• Give reassurance that the person has done the right thing by telling someone and inform parents.
• Make sure the person knows not to retaliate or return the message.
• Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
• Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
• Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the pupil who they have sent messages to.

All bullying incidents will be recorded and investigated in the incident log as any other bullying incident. We will then investigate fully as any other bullying incident.

Working in Partnership with Parents:

Parents/carers are asked to read through and sign acceptable use of ICT agreements on behalf of their child on admission to school (see appendices).

• Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website, SeeSaw and YouTube channel.)
• A partnership approach with parents will be encouraged. This includes parents' evenings with suggestions for safe home Internet use, advice on filtering systems and educational activities that include safe use of the Internet.

Appendix 1

ICT Acceptable Use Policy for pupils:

Agreement / eSafety Rules.

- I will take care when using the school IT equipment and use it properly
- I will only share my user name and password with trusted adults
- I will tell an adult if I see anything that upsets me
- I will make sure that when I communicate online that I am responsible, polite and sensible
- I will use a safe name and not my real name on the internet
- I know I am only allowed to go on the internet if my teacher has given me permission
- I will only take a photograph or video of someone if they say it is alright
- I will not deliberately write anything which upsets other people
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment
- I understand that if I do not follow these rules I may not be allowed to use the school computer, class iPad or internet for a while, even if it was done outside school

We have discussed this and …….... (child's name) agrees to follow the eSafety rules and to support the safe use of ICT at Egerton Primary School.

Parent / Carer Name (PRINT) ……

Parent / Carer (Signature) ……

Class …….. Date……

Appendix 2

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct:

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with a member of SLT.

• I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
• I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
• I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
• I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
• I will only use the approved, secure email system for any school business.
• I will not email documents giving details of pupils to external sources without password protecting the document first.
• I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
• I will not use or install any hardware or software without permission from the ICT technician.
• I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
• Images of pupils and/ or staff will only be taken with school devices, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or head teacher. I understand I cannot use my mobile phone to take photos of children.
• I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.
• I will respect copyright and intellectual property rights.
• I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
• I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name …….... (printed)

Job title: ……..

Appendix 3

Progression of skills and knowledge

Year Group		Strands		
		Computer Science	Digital Literacy (Inc. E-Safety)	Information Technology
KS1	1	Understand that an algorithm is a set of instructions used to achieve an objective. Know that an algorithm written for a computer is called a program. Work out what is wrong with a simple algorithm when the steps are out of order. Write a simple algorithm. When looking at a program, read code one line at a time. Create code using visual blocks. Know that an unexpected outcome is due to the code they have created. Make logical attempts to fix the code.	Understand what is meant by technology and identify a variety of examples both in and out of school. Make a distinction between objects that use modern technology and those that do not e.g. a microwave vs. a chair. Understand the importance of keeping information, such as their usernames and passwords, private (and actively demonstrate this in lessons). Take ownership of their work and save this in their own private space (such as their My Work folder on Purple Mash). Begin to make connections between the behaviours that keep us safe in the wider world and those that keep us safe online.	Show awareness of how adults carry out searches to retrieve digital content. Follow simple instructions to access online resources. Sort, collate, edit and store simple digital content e.g. name, save and retrieve our work. Create, name, save and retrieve content, with some support. Begin to use a range of media including photos, text and sound.
	2	Explain that an algorithm is a set of instructions to achieve an objective or to solve a problem. Show awareness of the need to be precise with algorithms so that they can be successfully converted into code. Create a simple program that achieves a specific purpose. Identify and correct some errors in a program. Display a growing awareness of the need for logical, programmable steps. Identify the parts of a program that respond to specific events and initiate specific actions.	Know the implications of inappropriate online searches. Begin to understand how things are shared electronically. Apply our learning on keeping personal information private to also describe how to use email safely. Consistently and correctly save their work in their own private space. Know how to report inappropriate behaviours and content to a trusted adult. Make connections between the behaviours that keep us safe in the wider world and those that keep us safe online.	Carry out simple searches to retrieve digital content. Apply learning of effective searching beyond the classroom. Organise data using a database and retrieve specific data. Edit more complex digital content such as music compositions or mind maps. Confidently create, name, save and retrieve content Use a range of media including photos, text and sound.

LKS2	3	Turn a simple real-life situation into an algorithm for a program by deconstructing it into manageable parts. Identify an error within a program that prevents it following the desired algorithm and then fix it. Design and code a program that follows a simple sequence, absorbing new knowledge of coding structures. Use timers to achieve repetition effects in their programs. Understand how variables can be used to store information while a program is executing. Attempt to 'step through' more complex code in order to identify errors in algorithms and then go on to correct this. List a range of ways that the internet can be used to provide different methods of communication through networking devices, e.g. email, social media and video calling.	Demonstrate the importance of having a secure password and not sharing this with anyone else. Explain the negative implications of failure to keep passwords safe and secure. Understand the importance of staying safe and the importance of their own conduct when engaging online. Know more than one way to report unacceptable content and contact. Use methods of online communication, e.g. being able to open, respond to and attach files to emails using 2Email. Describe appropriate email conventions when communicating in this way. Make increasing connections between our learning about physical and emotional safety in PSHE to our digital experiences.	Carry out simple searches to retrieve digital content, understanding that we are connecting to the internet and using a search engine such as Purple Mash search or internet-wide search engines. Collect, analyse, evaluate and present data and information using a selection of software. Consider what software is most appropriate for a given task and explain they conclusions. Create purposeful content to attach to emails relating or adding to the content within the message.
	4	When turning a real-life situation into an algorithm, use coding structures for selection and repetition. Make more intuitive attempts to debug their own programs. Become more logical and integrated when using of timers to achieve repetition effects. Understand 'if statements' for selection and attempt to combine these with other coding structures including variables to achieve the effects that they design in their programs. Use and manipulate the value of variables. Make use of user inputs and outputs such as 'print to screen'. Think of the structure of a program in logical, achievable steps and absorb some new knowledge of coding structures. Trace code and use step-through methods to identify errors in code and make logical attempts to correct this. In programs such as Logo, 'read' programs with several steps and predict the outcome accurately. Recognise the main component parts of hardware which allow computers to join and form a network.	Identify risks in password security and make steps to keep passwords safe and secure. Understand the online safety implications associated with the ways the internet can be used to provide different methods of communication is improving. Explore key concepts relating to online safety using concept mapping to help others to understand the importance of online safety. Know a range of ways of reporting inappropriate content and contact. Confidently make connections between lessons on physical safety in the world and apply these to prevent risks online. Begin to acknowledge that resilience is key to our emotional safety online, and we must prepare ourselves for being faced with content or experiences that might worry us.	Understand the function, features and layout of a search engine. Appraise selected webpages for credibility and information at a basic level. Make informed software choices when presenting information and data. Make improvements to digital solutions based on feedback. Create linked content using a range of software such as 2Connect and 2Publish+. Share digital content within their community, i.e. using Virtual Display Boards.

UKS2	5	Attempt to turn more complex real-life situations into algorithms for a program by deconstructing it into manageable parts. Test and debug programs as we go and use logical methods to identify the approximate cause of any bug (with some support). Translate algorithms that include sequence, selection and repetition into code with increasing ease. Create designs that show thinking of how to accomplish the set task in code utilising such structures. Combine sequence, selection and repetition with other coding structures to achieve their algorithm design. Beginning to think about code structure in terms of the ability to debug and interpret the code later, e.g. the use of tabs to organise code and the naming of variables. Identify examples of networking hardware in the devices at school and at home. Understand the value of networking together hardware but are also aware of the main dangers.	Recognise what personal information is and clearly and confidently explain how this can be kept safe. Select the most appropriate form of online communications contingent on audience and digital content, e.g. 2Blog, 2Email, Display Boards. Have a secure knowledge of common online safety rules and apply this by demonstrating the safe and respectful use of a few different technologies and online services. Implicitly relate appropriate online behaviour to our right to personal privacy and the mental wellbeing of ourselves and others. Confidently make connections between lessons on physical safety in the world; apply this learning and advise others on how to act in turn. Readily acknowledge that resilience is key to our emotional safety online, preparing to be faced with content or experiences that might worry us.	Search with greater complexity for digital content when using a search engine. Explain in some detail how credible a webpage is and the information it contains . Make appropriate improvements to digital solutions based on feedback received. Confidently comment on the success of the solution. Objectively review solutions from others. Collaboratively create content and solutions using digital features within software such as collaborative mode. Use several ways of sharing digital content, i.e. 2Blog, Display Boards and 2Email.
	6	Turn a more complex programming task into an algorithm by identifying the important aspects of the task (abstraction) and then decomposing them in a logical way. Test and debug program as we go, using logical methods to identify the cause of bugs. Show a systematic approach when identifying a particular line of code causing a problem. Consistently and correctly translate algorithms that include sequence, selection and repetition into code. Create designs that show thinking of how to accomplish the set task in code utilising such structures, including nesting structures within each other. Display an improving understanding of variables in coding, outputs such as sound and movement, and inputs from the user of the program such as button clicks and the value of functions. Understand and can explain in some depth the difference between the internet and the World Wide Web. Know what a WAN and LAN are.	Recognise what personal information is and make steps to keep it safe when presented with a “mock” real world scenario. Use critical thinking skills in everyday use of online communication. Consistently and competently, demonstrate the safe and respectful use of a range of different technologies and online services. Identify more discreet inappropriate behaviours through developing critical thinking, e.g. 2Respond activities. Recognise the value in preserving their privacy when online for their own and other people’s safety and act on this proactively and maturely. Confidently make connections between lessons on physical safety in the world; apply this learning and advise others on how to act in turn, taking on the role of digital leader as the oldest pupils in the school. Confidently describe how resilience is key to our emotional safety online, preparing to be faced with content or experiences that might worry us.	Explain in detail how credible a webpage is and the information it contains, making reference to “fake news” and the cross over between social media and news sources. Compare a range of digital content sources and rate them in terms of content quality and accuracy. Readily apply filters when searching for digital content. Utilise feedback as well as other criteria to evaluate the quality of digital solutions. Identify improvements, comment on its success and then build on this to create further refinements. Objectively review solutions from others, identifying elements that are beneficial and others that may not be. Make clear connections to the audience when designing and creating digital content. Design and create personal blogs to become a content creator on the internet, e.g. 2Blog.