John Ruskin Primary School and Language Classes

Computing Policy

Co-ordinator: Isabel Mattick, Jonathan Verity

Last review: January 2020
Next review: 2023

"**Be Responsible, be fair, stay positive and care**"

This policy should be read in conjunction with other policies including Anti-Bullying, Behaviour, PSHE, Child Protection, Data Protection, AUP and privacy notices.

Introduction

This policy aims to cover the different elements that Computing and Information and Communication Technology (ICT) can cover within our school. These guidelines have been drawn up to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum; this policy will enable these to go ahead. This policy will set out a framework for how Computing will be taught, assessed and monitored throughout the school and should reflect the ethos and philosophy of our school. This policy has been written with guidance and support from other teachers, schools and local authorities.

Aims/Rationale

Computing and ICT encompasses every part of modern life and it is important that our children are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world.

To enable all our staff and pupils to be confident, competent independent users and learners of Computing we aim:

- To use Computing where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- To use computing to help improve standards in all subjects across the curriculum
- To develop the competence and skills of pupils through Computing lessons and provide them with the chance to consolidate these in a cross-curricular context
- To ensure pupils are challenged in their use of Computing and are provided with exciting, creative ways in which to share their learning
- To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation
- To provide all staff with the training and support to ensure that they can, and have the confidence to, use computing to its full potential in all aspects of school life
- To use computing and technology as a form of communication with parents, pupils and the wider community

Curriculum

The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work, and how to put this knowledge to use through programming. Building on this knowledge and understanding, pupils are equipped to use computing to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through the use of technology – at a level suitable for the future workplace and as active participants in a digital world.

Computing will be taught across the curriculum and wherever possible, integrated into other subjects. There will be a need for stand-alone computing sessions to teach Computer Science skills that can then be applied in the cross-curricular sessions. There will be a selection of age-appropriate ideas on the network with links to lesson plans, how-to guides and examples to ensure teachers are able to fulfil the Computing curriculum. The Computing Coordinators will ensure that the plans provide coverage of the National Curriculum Programme of Study and that children are challenged and are able to succeed.

The National Curriculum Computing Programme of Study aims to ensure that all pupils:

- can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation
- can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems
- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems.
- are responsible, competent, confident and creative users of information and communication technology

Online Learning

As a school, we value the importance of providing opportunities for children to learn outside of school and we will provide these depending on the age of the child.

We will:

- Provide links to generic websites suitable for the age phase
- Provide links to websites suited to the current topic
- Participate in Computing and iPad reward sessions

Assessment

Computing will be assessed in a number of ways using formative and summative assessment. Formative assessment will happen during computing lessons and will be used to inform future planning and this is conducted by the teacher on an informal basis. Computing capability will be completed on a termly basis with work saved in a ‘best bits’ folder as an example. Children will complete age- appropriate self-assessments of work completed at the end of a topic.

As part of the summer term reports, teachers will provide parents with an indication of their children's progress so far as well as commenting on the child's progress and attainment in line with National Curriculum. Children will store their work on the network.

By the end of Key Stage 1 pupils should be taught to:

- understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions
- create and debug simple programs
- use logical reasoning to predict the behaviour of simple programs
- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

By the end of Key Stage 2 pupils should be taught to:

- design, write and debug 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
- use logical reasoning to explain how some simple algorithms work 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
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

Equal Opportunities and Inclusion

We will ensure that all pupils are provided with opportunities to access the Computing curriculum throughout the school. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to achieve.

Roles and Responsibilities - Senior Management Team

The head teacher and other members of the senior management team are responsible for monitoring the teaching of Computing throughout the school. The senior management team should decide on the provision and allocation of resources throughout the school in accordance to the school improvement plan, Computing action plans and timescales. They should also ensure that the Computing Coordinators and teachers are following their roles as listed below and in accordance to job specifications and performance management targets.

Roles and Responsibilities – Computing Coordinators

The Computing Coordinators will oversee planning in all year groups throughout the school and be responsible for raising standards in Computing. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The Computing Coordinators are responsible for overseeing the assessment of Computing across the school and providing opportunities to moderate Computing ability. The Computing Coordinators are responsible for managing equipment and providing guidance for future purchasing. The Computing Coordinators are also responsible for ensuring tools and procedures are sustainable.

Roles and Responsibilities - Teachers

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan and teach Computing and to use technology within their class. This will be in accordance to the schemes of work provided by the Computing Coordinators. They will also assist in the monitoring and recording of pupil progress in Computing. Teachers should also respond to, and report, online safety or cyber bullying issues that they encounter within or out of school in accordance to online safety procedures as listed below. Teachers should follow the e safety policy.

Whilst checking of personal sites, e.g. email, is permitted during non-contact times, staff should be aware that this should only happen for a brief time and that they should be extra vigilant and ensure they are logged off appropriately. Staff should follow, and agree to, the Acceptable Usage Policy.

Roles and Responsibilities - Governors and visitors

School governors should abide by the guidelines set out for staff and ensure that if they do use the computers and equipment within school that they are doing so safely. If either a visitor or governor wishes to have an account to logon to the school network, they should speak to a member of the senior management team.

Roles and Responsibilities - The School

As a school we will endeavour to ensure that parents and pupils are fully aware of ways in which the internet and technology can be used productively and safely. We will always ensure that we provide children with the opportunities to excel and achieve when using technology and will ensure our Computing curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through newsletters and parents events.

Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the AUP. They should ensure that they use the computers and equipment appropriately at all times.

It is expected that children will follow the school's behaviour policy when working online. They are also expected to adhere to the school's Anti-bullying policy. If the children fail to do so, then the procedures outlined in these policies will come into force.

Roles and Responsibilities - Parents

Parents should stay vigilant to the websites and content that their children are accessing. They should also try to talk to their child about e-safety and the use of the internet. If they have any questions or concerns then they should speak to their child's teacher, the Computing Coordinators or the head teacher.

Equipment, Hardware and Software

Hardware should not be installed without the permission of the head teacher and/or Computing Coordinators. All staff employed by John Ruskin should not be using memory sticks. Where exceptions have been made, they must use an encrypted memory stick provided by the Computing Coordinator for any school related documentation. Any sensitive data must be stored within the encrypted section.

The installation of software unauthorised by the school, whether licensed or not, is forbidden. If you are unsure, please speak to the head teacher and/or the Computing Coordinators for advice. The school reserves the right to examine or delete any files that are held on its system.

Network

Staff will be issued with a username for the computer and must choose their own password. Students will also be given log ins so that they can access documents and shared resources.

Backups

The data stored on the school's network is scheduled to a backup daily. This will allow backups of files to be recovered if the original becomes lost or damaged. Data is backed up via a cloud based system called Attix. The data is backed up in a data centre in Hoddesdon, HERTS and then mirrored to another secure data centre in a different geographical location. Data is encrypted at source.

Internet and E-mail

The internet may be accessed by staff and by children throughout their hours in school. We ask as a school that staff are vigilant as to the sites children are accessing and children should not be using the internet unattended – see AUP policy. Children who do not have permission to use the internet will not be allowed to access it at any time. All staff employed by John Ruskin have an LGfL or RMEasy Mail email account. This must be used for all school related correspondence; personal accounts must not be used for anything school related. Please discuss with Computing Coordinators and/or technician if you cannot access your account.

Age Limits

Certain online tools have age limits on the use of their software. This is due to an Act of United States Law. The Children's Online Privacy Protection Act prevents websites collecting data or providing their services to users under the age of 13.

As a school, we may decide to use some of these tools within lessons but will do so after thoroughly testing them for their safety and appropriateness. We will ensure that these will tend to be sites that allow creation of content rather than searching other users' content.

Occasionally these sites will be used by teachers with a class, for example to create a class book or movie, but not by a child with their own personal account. We will make parents aware of this during our e-safety events. If they do not wish their child to access these sites, their child can be provided with an alternative method to complete the task.

Personal Data

Staff should be aware that they should not transfer personal data such as reports, IEPs and contact information on to personal devices unless strictly necessary. This data should then be removed as soon as possible. When using a personal laptop or device containing student data, staff should be extra vigilant to not leave this device lying around or on display. Staff will be issued a home log-in to access the school network securely, only when strictly necessary.

Social Media

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. (See AUP Policy)

Digital and Video Images

As a school we will ensure that if we publish any photographs or videos of children online, we:

- Will try to ensure that their parents or guardians have given us written permission
- Will ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together without permission from the parents or guardians e.g. if the child has won an award
- Will ensure that children are in appropriate dress
- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher or to the Computing Coordinators. We will endeavour to remove the photograph as soon as possible
- Will provide new parents with a photo permission letter upon their arrival into school
- Will ask parents or guardians that are taking digital images at public events e.g. school play or sports day, that they do not publish these online. They will be asked not to record video.

If staff use personal cameras or phones to take photographs of children within school, these should be removed from the device as soon as possible. We are fully aware that this is necessary at times, but precautions should be taken to minimise the risks.

Technical Support

Many minor issues are dealt with by the Network Engineer and Computing Coordinators as appropriate. On site Hardware and Software technical support is provided every Monday by a network engineer from About Networks and works across the school depending on priority level. The engineer can be contacted via Outlook Messenger for emergency faults. There is remote monitoring of the school's network 24/7. Hardware and Software technical support is available remotely Monday to Friday 7.30am to 6.30pm. Any software or hardware issues can be recorded by raising a fault ticket by emailing support@aboutnetworks.co.uk and this is reviewed every day by the support desk. These faults will be resolved immediately (where appropriate) and reviewed by the Computing Coordinators and the school's Business Manager.

Online Safety

At John Ruskin we take Online Safety very seriously. We will ensure that it is taught often throughout the children's Computing and PSHE sessions as necessary. We will also provide children with dedicated online safety lessons. These will be reviewed regularly to ensure that they are up-to-date and reflect current needs. Children will be taught how to act online and how to minimise the risk when working on the internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them.

Our plans will provide children with an understanding of the expectations we have of them at a level appropriate to their age. We will also have an annual e-safety focussed children, staff and parent workshop and will provide regular updates via our website and newsletters as appropriate. The internet provides children and young people with access to a wide-range of content, some of which

is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used at our school block inappropriate content, including extremist content. Where staff, pupils or visitors find unblocked extremist content they must report it to the SPOC and complete a referral form.

All children will be taught about the Acceptable Use Policy and will sign a copy related to their age phase. These will be stored by the Computing and ICT Coordinators securely in pupil files. All staff will also complete an AUP. Useful ICT rules will also be posted in the Computing Room.

Online Safety training will also be provided for staff and governors to ensure that they conduct themselves in the appropriate manner when working and communicating online. If there is a website available to children that staff or children deem inappropriate they should speak to the Computing Coordinators who will then contact Southwark LA to attempt to get this blocked.

If a teacher suspects an online safety issue within school they should make notes related to the incident in accordance to anti-bullying, behaviour policies and child protection. This should then be reported to the Computing Coordinators and head teacher and recorded as appropriate.

Copyright and Intellectual Property Right (IPR)

Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the internet. Children will be taught in Key Stage 2 to begin to consider the use of images from the internet. In year 3/4 they will have discussions about the proper use of images with questions such as 'Is it OK to use an image we find online?' As they progress to year 5/6 some children should start referencing the sites they have used. This could be as simple as putting the name of the site the image came from or a hyperlink. It is not expected for children to include a full reference but to be *aware* that it is not acceptable to take images directly from the internet without some thought on their use.

All materials created by staff whilst in employment of the school belong to the school and should not be used for financial gain. This is in accordance with guidelines laid out by the local authority.

Responding to unacceptable use by staff

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.

Responding to unacceptable use by pupils

Pupils should be aware that all e-safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy and if necessary, the anti-bullying policy. Children may have restrictions placed on their account for a short time.

Monitoring, Evaluation and Review

The Computing Coordinators in consultation with the head teacher and staff will present the next review and evaluation of this document to the Governors for discussion and agreement on the effectiveness of this policy in February 2020**.**

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. **email, Internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, **equipment and systems.**

John Ruskin Primary School and Language Classes regularly reviews and updates all Acceptable Use Agreement (AUA) documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: [*LGfL StaffMail]*
- I will only use the approved *system* with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the E-safety lead.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the school's policy on use of mobile phones / devices at school.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

- I will only access school resources remotely (such as from home) using the *LGfL / school approved system* and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the safeguarding lead or deputy safeguarding leads if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the safeguarding lead or deputy safeguarding leads.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head* / *Safeguarding Lead* on their request.
- I understand that Internet encrypted content, may be scanned for security and/or safeguarding purposes.
- *Staff that have a teaching role only:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ……. .....Date.....

Full Name ..... (printed)

KS2 : Acceptable Use Agreement

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, laptops, iPads and everything else including cameras and other devices. By using the ICT in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them.

These rules will keep me safe and help me to be fair to others.

- At all times, I will think before I click (especially when deleting or printing)
- When using the internet, I will think about the websites I am accessing
- If I find a website or image that is inappropriate, I will tell my teacher straight away
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site
- When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will only use my first name and not share personal details that could identify me, my family or my friends, such as my email address or phone number
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not logon using another person's account without their permission
- I will think before deleting files
- I will think before I print
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using the computers and transporting equipment around
- I will keep my usernames and passwords private and secure, but I understand I can share them with appropriate people, such as my parents or teachers
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I am acting inappropriately then my parents may be informed

I have read and understand these rules and agree to them.

Signed (Pupil) _____ Class _____

Date _____

Key Stage 1: Acceptable Use Agreement

I keep **SAFE online** because …	✓
I **CHECK** it's OK to use a website / game / app.	
I **ASK** for help if I get lost online.	
I **THINK** before I click on things.	
I **KNOW** online people are really strangers.	
I am **RESPONSIBLE** so never share private information.	
I am **KIND** and polite online.	
I **TELL** a trusted adult if I am worried about anything.	

My trusted adults are:	Mum
	Dad
	Teacher

My name: Date signed:	