John Ruskin Primary School and Language Classes

Computing Policy

Co-ordinator: Owen Thompson

Last review: September 2024
Next review: September 2027

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

This policy should be read in conjunction with other policies including: E-Safety, Social Media, Anti-Bullying, Behaviour, PSHE, Child Protection, Data Protection, Acceptable Use Agreements 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 Computing curriculum is broken down into three main non-mutually exclusive strands. These are:

- Information and Communication Technology (ICT)
- Computer Science
- Digital Literacy

ICT is when we select, use and combine a variety of software (including internet services) on a range of digital devices to digest, manipulate or observe information. ICT is the 'skills based' aspect of Computing, the mechanics of actually using digital technologies correctly *i.e.,* using a keyboard and mouse/touch screen, typing correctly using punctuation, saving and accessing files on the school server *etc.*

When taught Computer Science, pupils learn the principles and practices of computation and computational thinking, and their application in the design and development of computer systems. Children learn how digital systems work through input > process > output, and the application of 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.

Digital Literacy is the ability and skill to find, evaluate, utilise, share, and create content using information technologies and the Internet. Just as the ability to read, spell, punctuate, and perform basic arithmetic, are essential life skills, so is the ability to use a computer. These lessons are essential to create safe, respectful, responsible, enthusiastic users of digital technologies. Key learning behaviours should be taught across PSHE and any other relevant curriculum areas. The school follows a newly devised Digital Literacy curriculum which was created to meet the requirements of the UK Council for Internet Safety framework as set out in *Education for a Connected World – 2020 edition A framework to equip children and young people for digital life.* The 8 key strands of this are:

- Self-Image and Identity
- Online Relationships
- Online Reputation
- Online Bullying
- Managing Online Information
- Health, Well-being and Lifestyle
- Privacy and Security
- Copyright and Ownership

This can currently be found in S:\All Staff Shared Data\Subjects\Computing\Digital Literacy\2023-24

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. It is advised that teachers aim to provide opportunity for one outcome per subject per half term to be created/presented/researched using digital technology.

The Computing curriculum is constantly reviewed by the Computing Coordinator. It is ensured that the units of work provide coverage of the National Curriculum Programme of Study and that children are challenged and are able to succeed. It is essential that teachers follow the units of work as set out in the Computing Curriculum Map – currently available here S:\All Staff Shared Data\Curriculum\3. Curriculum Maps\1. Subject Yearly Maps\Computing

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 those 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

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 may 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 and/or in any other relevant/secure online platform *e.g.,* Scratch, Book Creator, Code.org.

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 Leadership Team

The head teacher and other members of the senior leadership 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 Coordinator

The Computing Coordinator 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

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 Coordinator. 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 Agreement.

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 leadership 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, email and parents' events.

Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the Acceptable Use Agreements. 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 Coordinator or the head teacher.

Equipment, Hardware and Software

Hardware should not be installed without the permission of the head teacher and/or Computing Coordinator. 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 Coordinator 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 year group logins 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.

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. 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 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 Coordinator 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 Acceptable Use Agreements and the Social Media Policy (2024) for a more comprehensive overview.

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 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 Coordinator. 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 or videos at public events *e.g.,* school play or sports day, that they do not publish these online.

Staff should not use personal cameras or phones to take photographs of children within school, school equipment such as cameras and iPads should be used for this.

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 by a network engineer from Classroom365 who works across the school depending on priority level. 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 visiting https://support.classroom365.co.uk/support/tickets/new and this is reviewed every day by the support desk. These faults will be resolved immediately (where appropriate) and reviewed by the Computing Coordinator 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. In February each year, John Ruskin celebrates Safer Internet Day with assemblies and workshops delivered centring around a theme set by the UK Safer Internet Centre. Parents will be provided with online safety updates via our website, email and newsletters.

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 Agreement 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 Acceptable Use Agreement. Parents will also be sent an Acceptable Use Agreement and will be asked to read and adhere to this. They will also be sent the KS1 & KS2 agreements so they can better understand what their children have been asked to sign and adhere to.

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 Coordinator 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 Coordinator 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 and/or computer use for a short time.

Monitoring, Evaluation and Review

The Computing Coordinator 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 September 2027.

JOHN RUSKIN PRIMARY SCHOOL

Acceptable Use Agreement for KS1 Pupils

LGfL SafeguardED

My name is _____ Date:_____

I keep **SAFE online and on my devices,** because…	✓
I only **USE** devices or apps, sites or games if I am allowed to	
I **TELL** a trusted adult if I'm upset, worried, scared or confused	
I look out for my **FRIENDS** and tell someone if they need help	
I **KNOW** that online people aren't always who they say they are	
I understand that things I read online are not always **TRUE**	
Anything I do online can be shared and might stay online **FOREVER**	
I don't keep **SECRETS** 🚫 unless they are a present or nice surprise	
I don't have to do **DARES OR CHALLENGES** ❌	
I don't change **CLOTHES** or get undressed in front of a camera	
I always check before **SHARING** my personal information	
I ask **PERMISSION** before sharing other people's stories and photos	
I am **KIND** and polite to everyone	

My trusted adults are:

_____ at school

_____ at home

_____ at _____

Acceptable Use Agreement for
KS2 Pupils

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about Computing and ICT, we are talking about computers, laptops, iPads, smartphones 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 statements can keep me and others safe & happy at school and home

1. ***I learn online*** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things.
5. ***I am a good friend online*** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something fun, a joke or 'banter' doesn't stop it hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
11. ***If I make a mistake I don't try to hide it but ask for help.***
12. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
13. ***I know online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
14. ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.

15. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
16. ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
17. ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
18. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
19. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
20. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
21. ***I follow age rules*** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
22. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
23. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
24. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
25. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
26. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
27. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, and I know which sites to trust, and how to double check information I come across. If I am not sure I ask a trusted adult.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult:

at school that might mean _____

Outside school, my trusted adults are_____

Signed: _____ **Date: _____**

Acceptable Use Agreement for Parents/carers

Background

We ask all children, young people and adults involved in the life of John Ruskin Primary School to read and sign an Acceptable Use Agreement to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an Acceptable Use Agreement which is kept digitally on file at school.

We tell your children that **they should not behave any differently when they are out of school or using their own device or on a home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school. We seek the support of parents and carers to reinforce this message and help children to behave in a safe way when online:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read John Ruskin's full Online Safety Policy on the school website for more detail on our approach to online safety and links to other relevant policies (e.g., Safeguarding and Child Protection Policy, Behaviour Policy, etc). If you have any questions about this Acceptable Use Agreement or our approach to online safety, please contact the office.

What am I agreeing to?

1. I understand that John Ruskin uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.
3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to 'overblock' or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school is subject to filtering and monitoring.
5. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.

6. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
7. Children are not allowed mobile phones and/or devices in schools. Parents are kindly reminded that urgent messages can be passed via the school office.
8. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
9. I will follow the school's Social Media policy which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
10. I understand that for my child to grow up safe online, they will need positive input from school and home, so I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content *etc.*
11. I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
12. If my child has online tuition, I will refer to the Online Tutors – Keeping children Safe poster and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.
13. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet and to various devices, operating systems, consoles, apps and games. There are also child-safe search engines e.g. kiddle.co and YouTube Kids is an alternative to YouTube with age appropriate content. Find out more at parentsafe.lgfl.net
14. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
15. I understand and support the commitments made by my child in the Acceptable Use Policy (Acceptable Use Agreement) which they have signed, and I understand that they will be subject to sanctions if they do not follow these rules.
16. I can find out more about online safety at John Ruskin by reading the full Online Safety Policy, available on the school website.
17. If I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school, I can talk to school leadership.

Acceptable Use Agreement for
Staff, governors & volunteers

Background

We ask everyone involved in the life of John Ruskin Primary School to sign an Acceptable Use Agreement, which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This agreement will be reviewed annually, and staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

If you have any questions about this agreement or our approach to online safety, please speak to the Computing lead.

What am I agreeing to?

1. **(This point for staff and governors):**
   I have read and understood John Ruskin's full E-Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the E-Safety Policy.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area.
3. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead and make them aware of new trends and patterns that I might identify.
4. I will follow the guidance in the Safeguarding and E-Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media)
5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.
6. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'!
7. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language
8. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHE and SRE curriculum, both outside the classroom and within the curriculum, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

9. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
10. I will follow best-practice pedagogy for online-safety education, avoiding scaring and other unhelpful prevention methods.
11. I will prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
12. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.
13. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main safeguarding policy when it comes to behaviour.
14. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
15. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE 2023. If I discover pupils may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay.
16. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
17. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
18. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full E-Safety and Social Media policies. If I am ever not sure, I will ask first.
19. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
20. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
21. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Agreements and will report any infringements in line with school procedures.

22. I understand that breach of this Acceptable Use Agreement and/or of the school's full E- Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this agreement. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent E-safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____