John Ruskin Primary School and Language Classes

Online Safety Policy

Co-ordinator: Owen Thompson

Last review: September 2024
Next review: 2027

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

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at John Ruskin School and Language Classes with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content
- Effective searching and critical evaluation of data

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

- Giving and denying consent (in regards to use of their personal image, details, data etc.)

Scope

This policy applies to all members of John Ruskin School and Language Classes community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of John Ruskin School and Language Classes.

Roles and responsibilities

Please read the relevant roles and responsibilities section from the following pages.

All school staff must read the "All Staff" section as well as any other relevant to specialist roles

Roles:

- All Staff
- Headteacher
- Governors
- PSHE / RSHE Lead/s
- Computing Lead
- Network Manager/technician
- Teachers
- Pupils
- Parents/carers
- External groups including Parent groups

Role	Key Responsibilities
All staff, volunteers and contractors.	• Read, understand, sign and adhere to an Acceptable Use Agreement • Report any concerns, no matter how small, to the designated safety lead • Maintain an awareness of current online safety issues and guidance • Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications

Role	Key Responsibilities
Headteacher	*As listed in the 'all staff' section, plus:* • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, *e.g.,* LGfL services • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
Governors	*As listed in the 'all staff' section, plus:* • To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities
Computing Lead	*As listed in the 'all staff' section, plus:* • To oversee the delivery of the newly revised digital literacy element of the Computing curriculum • Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements • To provide information for parents about relevant issues related to computer use in and outside of school (digital wellbeing, social media, digital footprint *etc.*)
Network Manager/technician	*As listed in the 'all staff' section, plus:* • To manage the school's computer systems, ensuring - systems are in place for misuse detection and malicious attack (*e.g.,* keeping virus protection up to date) • To ensure appropriate backup procedures and disaster recovery plans are in place
Teachers	*As listed in the 'all staff' section, plus:* • To embed online safety across throughout their practise by modelling safe, responsible and professional behaviours in their own use of technology • To deliver explicit online safety lesson following the newly revised digital literacy curriculum; following the Medium-Term Plans for their respective year group • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills (children to use www.kiddl.co for searching the internet) and are fully aware of legal issues relating to electronic content such as copyright laws

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the KS1/KS2 Acceptable Use Agreement • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school
Parents/carers	• Read and adhere to the school's parental Acceptable Use Agreement and encourage their children to follow it • to consult with the school if they have any concerns about their children's use of technology • To accentuate the importance of online safety to their children modelling safe, responsible, respectful and positive behaviours in their 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
External groups including Parent groups	• Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school • Support the school in promoting online safety and data protection • Model safe, responsible, respectful and positive behaviours in their 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

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staffroom/ classrooms.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear and newly devised, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, *e.g.,* use of passwords, logging-off, use of content, research skills, copyright, digital footprint;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;

Parent awareness and training

This school:

- runs a rolling programme of online safety advice, guidance and/or training for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand-held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Incident Management

In this school:

- support is actively sought from other agencies as needed (*i.e.,* the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all adult users
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services;
- Has daily back-up of school data;

To ensure the network is used safely, this school:

- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

E-mail

This school:

- Provides staff with an email account for their professional use, London Staffmail/LA email and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Will use the email system provided by LGfL for all school emails. Staff never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

Social networking

For a more complete overview of the school's policy on social networking, please refer to the Social Media Policy (2024).

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- All staff are DBS checked and records are held in a single central record

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
- All mobile devices will be handed in at reception should they be brought into school.
- Personal mobile devices will not be used during lessons or formal school time.
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at another time than their break times.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices

- The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety, however the school strongly advises that student mobile phones and devices should not be brought into school.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually).;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long-term, high-profile use
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their

location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

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: _____