St John of Jerusalem
Church of England Primary School

COVID 19

Remote Learning Protocol Policy

1. Remote Learning and Acceptable Use

Table of Contents

a. Introduction

Advancement in technologies now means that St John of Jerusalem school has an online platform to facilitate remote learning. This opens up all sorts of learning possibilities for our pupils, reflecting our values with regards to inclusion and access to learning.

This policy supports the school's commitment to safeguarding pupil and staff.

b. Remote Learning

Any teaching staff seeking to use the Learning Platform to deliver remote learning to pupils must inform the Deputy Head Teacher.

Lessons to be delivered must follow the school curriculum, and teachers are required to include a summary of the lesson objectives and contents in their lesson plan. All lessons delivered through this platform must be accessible by the SLT. A member of the SLT will be assigned to each class and will be given access to join the streaming session at any point.

Teachers must familiarise themselves with the Twenty Safeguarding Considerations for Lesson Live streaming – (see appendix 4)

The school network or a school device must be used for the purposes of streaming lessons. When planning lessons to be streamed from home, teachers must ensure only approved websites are accessed and that the laptop setting prevents pop-ups (that may be inappropriate).

c. Acceptable Use

Staff and Pupils are required to sign the acceptable use policy before accessing the platform and live streaming lessons (Live Streaming must be approved in advance by a member of the SLT).

The objectives of this policy for remote access by staff are:

- To provide secure and resilient remote access to the school's information systems.
- To preserve the integrity, availability and confidentiality of the school's information and information systems.
- To manage the risk of serious financial loss, loss of stakeholder confidence or another serious business impact which may result from a failure in security.
- To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the school is adequately protected under computer misuse legislation.

d. User Responsibilities, Awareness & Training

The School will ensure that all users of information systems, networks, teaching platforms and applications are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. Irresponsible or improper actions may result in disciplinary action(s).

All users are required to:

- Read this policy and sign the acceptable use agreement form.
- Record all live streaming sessions and to save this in the 'Live Recordings' folder which is accessible by all members of the SLT.
- Ensure they regularly change their network and school laptop passwords; ensure this is a strong password and that this is not shared with others.
- Agree to only access the school network via a school owned device e.g. laptop.
- Follow good practice in regards to software updates, including anti-virus and ensure the school's designated technician inspects the device at least annually or when a virus or malware is suspected. The device must not be used until this has been removed.
- Only access the School network in a secure, private location i.e. never in a public place.
- Mobile devices are not left unattended, or that data that is deemed confidential is not left visible on the screen.
- Not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication or access information that is not relevant to their role.
- In order to avoid confusing official company business with personal communications, employees with remote access privileges must never use non-school e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct school business.

- The remote access user also agrees to report immediately, to their manager and to the SLT any incident or suspected incidents of unauthorised access and/or disclosure of school resources, databases, networks, etc.
- The remote access user also agrees to and accepts that his or her access and/or connection to St John of Jerusalem school's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity.

e. Removal of Remote Learning Rights

The school reserves the right to withdraw this facility from users at any time if they are in breach of the conditions of use, or where their actions have compromised the safety of others or have led to a breach of confidentiality, integrity/or availability of the school's systems or services.

The remote access rights of all employees and third party users shall be removed upon termination of employment, contract, or agreement and all School owned systems and other devices, and information/data must be returned to St John of Jerusalem School upon the termination of employment or contract.

f. Next steps

1. Please complete, sign and return the acceptable use agreement and remote access checklist.
2. Ensure that your school laptop/device has received an annual health-check and is fully updated.
3. Collect your remote access user guide and login instructions from the Admin Manager.

This policy is to be read alongside the:

- Computing Policy
- Online Learning Policy
- Safeguarding Policy
- Data Protection Policy
- Remote Access Policy

This policy was ratified by the Standards, teaching and Learning Committee on TBC

Date of the next Review: Spring 2021

g. Appendix 1 - Acceptable use policy (STAFF)

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct
This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Patricia Lewis, school e. safety coordinator.

1. I have read and understood St John of Jerusalem COE Primary School's full Online Safety policy at https://www.st-johnjerusalem.hackney.sch.uk 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.

2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult). DSL (René Africa and Carly Richards) HT (Asarena Simon).

3. During remote learning:

- I will not behave any differently towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
- I will not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.
- I will not take secret recordings or screenshots of myself or pupils during live lessons.

- I will conduct any video lessons in a professional environment as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
- I will complete the issue log for live lessons if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students

4. I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.

5.I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the RSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.

6.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.

7. 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, including social media, e.g. by:

- not sharing other's images or details without permission
- refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

8. 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, which are detailed in the school's Online Safety Policy. Our policy can be read on our website; https://www.st-johnjerusalem.hackney.sch.uk I will report any breach of this by others or attempts by pupils to do the same to the headteacher.

9. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am unsure whether I am allowed to do something in or related to school, I will seek advice from the SLT.

10. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair any of them. More guidance on this point can be found in this Online Reputation guidance for schools and in St John of Jerusalem COE Primary School's social media policy/guidance.

11. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the Head/ Deputy Head teacher if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.

12. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, if allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

13. 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.

14. 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 by the school.

15. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

16. I will follow the guidance in the safeguarding and online-safety policies for reporting incident: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handling incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.

17. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

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

Signature …….…… Date ……

Full Name …….…… (Printed)

h. Appendix 2 - Acceptable use policy (PUPILS & PARENTS)

St John of Jerusalem Acceptable ICT Use Agreement for Pupils & Parents

✓ Acceptable Use Agreement / e-Safety Rules

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and:

1. I only **USE** devices or apps, sites or games if a trusted adult says so.
2. I **ASK** for help if I'm stuck or not sure.
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused.
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult.
5. I look out for my **FRIENDS** and tell a trusted adult if they need help.
6. I **KNOW** people online aren't always who they say they are.
7. I understand that anything I do online can be shared and might stay online **FOREVER.**
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to.
9. I don't change **CLOTHES** or get undressed in front of a camera.
10. I always check with a trusted adult before **SHARING** personal information.
11. I am **KIND** and polite to everyone.

ICT, including the internet, email and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and sign and return to the school office. If you have any concerns or would like some explanation, please contact the Deputy Headteacher.

Remote Learning

I understand that St John of Jerusalem School may on occasions use technology to support home learning. These sessions will always be pre-planned and I will ensure that a responsible adult is within the vicinity.

I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies.

I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media.

I will follow the school's acceptable use policy and on-line safety 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.

I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.

I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/

I understand and support the commitments made by my child in the Acceptable Use Policy (AUP), which can be seen above.

We have discussed the Acceptable Use Agreement / e-Safety Rules with our child, and they agree to follow the e-Safety rules and to support the safe use of ICT at St John of Jerusalem School and home.

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____

i. Appendix 3 - Remote Learning Check List (Staff)

	Please sign below
I have read and am aware of my duties under the remote learning policy	
I have read and am aware of my duties as regards the Twenty Safeguarding Considerations for Lesson Livestreaming	
I have read, signed and returned the acceptable use agreement form	
I have received training and advice on how to safely offer remote learning to pupils	
I have ensured that my school laptop is fully updated and has had an annual health check	
I have ensured that software updates are automatic	
I have created a strong password and that passwords are not automatically saved on my device	
I am aware that I must pre-plan all remote streaming sessions and obtain the necessary permission for this to go ahead.	
I am aware that I must advise parents/carers of the date and time of the session in advance	
I have set up a 'guardian invitation' for each pupil so that they will receive regular updates on lessons streamed and work provided.	
I will ensure that all live streaming sessions are recorded and that this is saved in the 'live recordings' shared folder	
I am aware of the requirements of the staff code of conduct and will abide by this	

Completed by:

Print name:

Date:

For office use: (initial and date when completed)

Acceptable use policy and remote access agreement signed and to be filed in staff file

Training session on remote Learning, including safety protocols attended

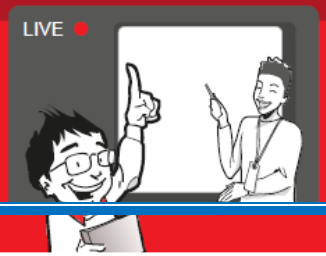
Remote Learning guidance and login details supplied

j. Appendix 4 – Twenty Safeguarding Considerations for Lesson Livestreaming

Twenty Safeguarding Considerations for Lesson Livestreaming

Just because schools are supporting students remotely and sending work home does NOT mean that you need to livestream lessons. This should only be done where you are equipped to do so safely. But if you are considering it, bear these things in mind:

1. Only use school-registered accounts, never personal ones
2. Don't use a system that your SLT has not approved
3. Will some students be excluded? Do they have internet, a device and a quiet place?
4. Do students and staff have a safe and appropriate place with no bedrooms or inappropriate objects/information visible?
5. Check the link in an incognito tab to make sure it isn't public for the whole world!
6. Has your admin audited the settings first (who can chat? who can start a stream? who can join?)
7. What about vulnerable students with SEND and CP needs?
8. Don't turn on streaming for students by mistake – joining a stream ≠ starting a stream
9. Never start without another member of staff in the 'room' and without other colleagues aware
10. Once per week may be enough to start with – don't overdo it and make mistakes.
11. Keep a log of everything - what, when, with whom and anything that went wrong
12. Do you want chat turned on for pupils? Can they chat when you aren't there?
13. Avoid one-to-ones unless pre-approved by SLT
14. Remind pupils and staff about the AUP agreements they signed* The rules are the same
15. Remind pupils and staff about the safeguarding policy and reporting process – does it work remotely?
16. Do you want to record it? Are students secretly recording it? You may not be able to tell.
17. How can students ask questions or get help?
18. What are the ground rules? When can students speak / how?
19. If you don't understand the system, if it won't be safe or reliable, if teaching won't be enhanced, DON'T DO IT.
20. Is your DPO happy? GDPR covered? Parental consent needed?



LGfL DigiSafe *keeping children safe*

THE DIGISAFE TEAM WILL BE EXPLORING SAFE SETTINGS FOR THE MAIN PLATFORMS
CHECK OUR SOCIAL PAGES
@LGfLDigiSafe

* Need templates?