Kingsway Infant School

Online Safety Policy – Acceptable Use Agreements

Appendices

A. Online Safety Acceptable Use Agreement - Staff, Governors and Student Teachers (on placement or on staff)

B. Online Safety Acceptable Use Agreement - Peripatetic Teachers/ Coaches, Supply Teachers

C. Online Safety Acceptable Use Agreement - Requirements for Visitors and Adult Helpers (Volunteers) Working in the School (working directly with children or otherwise)

D. Online Safety Acceptable Use Agreement - Primary Pupils

E. Guidance on the Process for Responding to Cyberbullying Incidents

F. Guidance for Staff on Preventing and Responding to Negative Comments on Social Media

G. Online Safety Incident Reporting Form

H. Online Safety Incident Record

I. Online Safety Incident Log

J. Safeguarding and Remote Education during Coronavirus (COVID-19)

Appendix A

Online Safety Acceptable Use Agreement - Staff, Governors and Student Teachers (on placement or on staff)

You must read this agreement in conjunction with the Online Safety Policy and the Data Protection (GDPR) policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that **all** Staff and Governors are aware of their responsibilities in relation to their use. All Staff, Governors and Student Teachers are expected to adhere to this agreement and to the Online Safety Policy. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and Police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information that may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the Online Safety Lead and/or DSP (Designated Senior Person) and an incident report completed.

Online Conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see Online Safety Policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social Networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, Governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data Protection

I will follow requirements as outlined in Data Protection (GDPR) policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely.

- Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.

- Personal or sensitive data taken off site must be encrypted.

Images and Videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of Email

I will use my school email address or GovernorHub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email address or GovernorHub for personal matters or non-school business.

Use of Personal Devices

I should at no time, as a member of staff, put myself in a position where a safeguarding allegation can be made against me because of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school. Such a system would ensure as the user that I was not saving files locally to my own device and breaching data security.

I will ensure I use a secure password/passcode when accessing school emails and data.

Under no circumstance will I contact a pupil or parent/carer using my personal device.

Additional Hardware/Software

I will not install any hardware or software on school equipment without permission of the Headteacher.

Promoting Online Safety

I understand that online safety is the responsibility of all staff and Governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, Governors, visitors, pupils or parents/carers) to the Headteacher and/or DSP.

Classroom Management of Internet Access

I will pre-check for appropriateness all internet sites used in the classroom, this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues, I will secure on every occasion, approval in advance for the material I plan to use with the Headteacher.

Video Conferencing

I will only use the conferencing tools that have been identified and risk assessed by the Headteacher, DSP and DPO. A school-owned device should be used when running video-conferences, where possible.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a Governor.

Signature: …… Date: ……

Full Name: …….... (block capitals)

Job Title/Position: ……

Appendix B

Online Safety Acceptable Use Agreement - Peripatetic Teachers/Coaches, Supply Teachers

Kingsway Infant School

Online Safety Lead: Debbie Knights

Designated Safeguarding Lead (also known as DSP - Designated Senior Person): Debbie Knights
Deputies - Donna Byrne and Fran Rogers

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain a copy for your own reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that **all** Staff and Governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and Police involvement will be sought.

The school's Online Safety Policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information that may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the Online Safety Lead and/or DSP and an incident report completed.

Online Conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see Online Safety Policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Online Safety Lead.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers. Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Headteacher.

Social Networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, Governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data Protection

I will follow requirements as outlined in Data Protection (GDPR) policy. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.

- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and Videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be only used for this purpose.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and

parent/carer's agreement on a school device, an organisational device approved by the Headteacher/DSP.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of Personal Devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices at home if allowed by the school and with parent/carer agreement.

Under no circumstance will I contact a pupil or parent/carer using my personal device.

Additional Hardware/Software

I will not install any hardware or software on school equipment without permission of the Headteacher.

Promoting Online Safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, Governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the Headteacher and/or DSP.

Classroom Management of Internet Access

I will pre-check for appropriateness all internet sites used in the classroom/tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues, I will secure, on every occasion, approval in advance for the material I plan to use with the Headteacher.

Video Conferencing

I will only use the conferencing tools that have been identified and risk assessed by the Headteacher, DSP and DPO. A school-owned device should be used when running video-conferences, where possible

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature: …… Date: ……

Full Name: …… (block capitals)

Company Name/Job Title/Role:……

Appendix C

Online Safety Acceptable Use Agreement

Requirements for Visitors and Adult Helpers (Volunteers) Working in the School (working directly with children or otherwise)

Kingsway Infant School

Online Safety Lead: Debbie Knights

Designated Safeguarding Lead (also known as DSP - Designated Senior Person): Debbie Knights
Deputies - Donna Byrne and Fran Rogers

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the Headteacher and/or DSP.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.

- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.

- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the Headteacher/DSP is informed before I leave the school.

- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared on line, including on social media sites.

- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher. If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school or the Headteacher.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in school.

Signature: …… Date: ……

Full Name: …… (block capitals)

Company Name/Job Title/Role: ……

Appendix D

Online Safety Acceptable Use Agreement - Primary Pupils

My Online Safety Rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.

- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.

- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.

- I understand my behaviour in the virtual classroom should mirror that in the physical classroom.

- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.

- I understand that these rules are designed to keep me safe now and in the future. If I break the rules, my teachers will look into it and may need to take action.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with the Headteacher.

Please return the signed sections of this form, which will be kept, on record in school.

Online Safety Acceptable Use Agreement - Primary Pupils

Pupil Agreement

Pupil Name: ……..……..…..…

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil Signature: ……..……..

Parent(s)/Carer(s) Agreement

Parent(s)/Carer(s) Name(s): ……

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information, images online, or post material that may bring the school or any individual within it into disrepute. Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents.

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent/Carer Signature: ……..……..

Date: ……..…..…

Appendix E

Guidance on the Process for Responding to Cyberbullying Incidents

All cyberbullying incidents should be reported. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.

- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, Headteacher) and staff members should seek support from their line manager or a senior member of staff.

- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded, as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the Police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.

- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.

- A senior member of staff will conduct an investigation.

- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary, the Police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix F

Guidance for Staff on Preventing and Responding to Negative Comments on Social Media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents/carers can use a school's social media site as a source of reliable information. The Online Safety Policy, see Appendix 1 (Summary of Key Parent/Carer Responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families, children and the community. Parents/Carers should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- **Collect the Facts**

  As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings, they are secured and retained together with any other evidence. Do not become engaged in responding directly.

  If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the Police, and the Headteacher will need to follow the school's safeguarding procedures.

  If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

  Adverse comments of any kind are highly demotivating and can cause stress and anxiety. It is important that senior staff reassure and support all staff and/or other affected members of the school community.

- **Addressing Negative Comments and Complaints**

  Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

  The meeting must:

  - Draw attention to the seriousness and impact of the actions/postings;
  - Ask for the offending remarks to be removed;
  - Explore the complainant's grievance;
  - Agree next steps;
  - Clarify the correct complaints procedures.

  If the meeting does not resolve the issue, the parents/carers must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the Police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix G

Online Safety Incident Reporting Form

Any member of the school community can raise a concern about an Online Safety Incident. If you have witnessed or experienced an incident, please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to the Online Safety Lead/Headteacher/DSP.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement, please specify:			

Continued, page 1 of 2.

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, WhatsApp, Snapchat, Instagram etc.
Evidence of the incident	Specify any evidence available but do not attach.

Thank you for completing and submitting this form.

Appendix H

Online Safety Incident Record

Name of person reporting incident:				
Date of report:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement, please specify.			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, WhatsApp, Snapchat, Instagram etc.
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to Online Safety Lead/Headteacher/ DSP	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to Police and/or CEOP	
Online Safety Policy to be reviewed/amended	
Parent(s)/Carer(s) informed, please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix I

Online Safety Incident Log

Summary details of ALL online safety incidents will be recorded on this form by the Online Safety Lead or other designated member of staff. This incident log will be monitored at least termly and information reported to the Senior Leadership Team (SLT) and Governors.

Date & Time	**Name of pupil or staff member** Indicate target (T) or offender (O)	**Nature of Incident(s)**	**Details of Incident** (including evidence)	**Outcome** including action taken

Appendix J

Safeguarding and Remote Education during Coronavirus (COVID-19)

Useful Resources

Below are resources (please note: not an exhaustive list) to help schools manage and risk assess any remote teaching and working.

Government guidance on safeguarding and remote education

https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

The Key for School Leaders - Remote learning: safeguarding pupils and staff

https://schoolleaders.thekeysupport.com/covid-19/safeguard-and-support-pupils/safeguarding-while-teaching/remote-teaching-safeguarding-pupils-and-staff/?marker=content-body

NSPCC Undertaking remote teaching safely

https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely

LGfL Twenty safeguarding considerations for lesson livestreaming
https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

swgfl Remote working a guide for professionals
https://swgfl.org.uk/assets/documents/educational-professionals-remote-working.pdf

National Cyber Security Centre Video conferencing. Using services securely
https://www.ncsc.gov.uk/files/vtc_infographic.pdf