ST NICHOLAS SCHOOL

ONLINE SAFETY POLICY APPENDIX: Live-Streamed Digital Lessons and Meetings guidance

INTRODUCTION

This policy appendix was developed by the Stephen King (Online Safety Co-ordinator/Deputy DSL) in consultation with the whole teaching staff. This policy appendix was introduced as a result of the school introducing live-streamed lessons and communications with pupils and their families in response to COVID-19 and is now a part of our home learning offer. This policy appendix has been agreed by the Senior Leadership Team and has been approved by the Governing Body. It is reviewed annually.

Since the Covid-19 school closure and phased re-opening, St Nicholas School has begun delivering online learning & video conferencing lessons. We use 3 secure video conferencing platforms Microsoft Skype for Business, Microsoft Teams and/or Zoom. Staff and students taking part will need to abide by all school/class rules and follow the guidance of the document: "National Online Safety - A Guide to Safer Live Lessons" (attached). Members of the STLS are also involved in digital communications with other schools, parents and NHS colleagues, they too should follow this policy and its advice, where applicable.

POLICY INTO PRACTICE

General Advice for Teachers/Hosts in planning lessons or liaising with families

o   All live-streamed digital lessons and/or meetings should be planned to take place within and restricted to reasonable hours (during the time of the school day). Where possible, pre-record content (videos/PowerPoints)

o   Ensure that (especially during the COVID-19 phase-return) staff look after themselves, keep reasonable deadlines and maintain a reasonable working hours- so as to provide a good work-life balance

o   When speaking to parents ensure that a school phone is used or that the personal phone number is withheld (using 141 before dialling). Staff are not to log the phone numbers of families (for GDPR purposes) or pupils (for safeguarding purposes) in the contact lists of their personal mobile phones

o   Should any member of staff become aware of any unkind or inappropriate chat/comments between students (during any digital lesson or communication) then please follow the school procedures for Positive Behaviour Support and contact the Extended/Senior Leadership Teams or the parents/carers, as necessary

o   If staff are delivering a live-streamed lesson from their own home, ensure that any unsuitable or personal items are not visible, a 'neutral' background is visible and that other adults from their household cannot hear/be seen/take part in events (for confidentiality and safeguarding purposes). Staff's own children may (need) to be present for their own family safeguarding and supervision purposes, this is permitted and allows for inclusion.

o   The school dress code must be followed at all times to ensure professionalism

o   Staff should plan to mute and/or disable learner's videos and microphones, as required

Online Safety away from school (Staff)

It is vital with homeworking that school staff:

o   Only use registered school email accounts, MS One Drive, MS Skype for Business or MS Teams – staff are not permitted to use personal accounts. If staff member sets up a Zoom account for use in live-streamed lessons, the username must be their school email address. The NOS guidance "A guide to safer live lessons" must be followed in Zoom, Skype or Teams Live lessons. ALL SESSIONS MUST BE PLANNED APPROPRIATELY (ACCORDING TO THE APPROPRIATE CURRICULUM POLICY) WITH DATE/TIMINGS SHARED WITH SLT AND PARTICIPANTS VIA EMAIL, IN ADVANCE

o   Should be professional in their manner and use appropriate language at all times – pupils and (potentially) parents/carers will be taking part and the staff code of conduct will apply in all digital

interactions
- o Please report any incidents that take place using the correct incident form – Behaviour, CP, Anti-Bullying, Racial or Online Safety
- o Remember the guidance of our Acceptable Use policies
- o Record all live-streamed sessions, uploaded them onto OneDrive, report any concerns and delete recorded files after 30 days - see Data Security and Online Safety Rules (below)
- o Plan to include at least one other staff member to be present during the live video session so there can be support and an independent staff witness to the events, at the time. This complies with our lone working policy. Prior SLT approval and a written rationale must be provided for any occasion where a teacher/host wishes to deliver a single staff lesson
- o Live-streamed lessons that are 1-1 (1 staff member and 1 child) should be avoided where possible due to the safeguarding implications. In some exceptional circumstances a 1-1 session may be appropriate (e.g. in a therapeutic setting) – increased safeguards would be recording the session, sharing the recording with the parent/allowing them to record at their end, sharing the recording with additional staff members, permission for a 1-1 session from the parent in advance, potential additional staff/family members being present in or part of the call, to mitigate the risks.
- o Have appropriate methods of responding to pupil or parent questions and can offer support
- o Should consider whether the lesson needs pupils' cameras to be on - would a sound-only session suffice?
- o Ensure that any YouTube, files or video/audio clips are age appropriate and monitored closely to the end (to be certain that they do not contain any harmful content – this must be reported to the UK Safer Internet Centre – www.saferinternet.org.uk
- o Ensure that staff have appropriate privacy on their devices and follow GDPR and school privacy notice guidance.
- o Share any concerns of a Safeguarding nature should be raised with a DSL immediately.
- o Share any potential conflicts of interest which may arise between staff and families with the SLT, prior to a live streamed lesson.

Data Security and Online Safety Rules for staff, students and families.

Online lessons will be delivered in closed user groups, and therefore are not available to those who have not been approved by the school – all participants will be invited using secure and official school email addresses.

Staff, students, parents and carers wish to engage in digitally-streamed lessons must agree to the following rules:

- All computer/mobile devices used to conduct the session must be kept up-to-date with their necessary anti-virus and threat protection definitions.
- The latest software version of the video conference platform/mobile App must be used.
- The teacher (host) will set the privacy controls so that screen sharing is limited to them only.
- File transfers will be turned off to reduce any risk of hacking or installing a virus/malware.
- The video conference meeting will be created/planned using a strong password which incorporates letters, numbers and symbols.
- The meeting will be set up with a waiting room (if appropriate), so that each authorised participant has to be admitted by the teacher hoSt
- The video session must be locked after 3 minutes (if appropriate) so that additional participants cannot (request to) join or be admitted once the lesson is in progress.
- It is desirable for parent/carer be present in the room when pupils are engaging in an online lesson.
- All participants (teachers/pupils/parents or carers) must be respectful to each other and observe the school rules to ensure a 'safe' learning environment.
- Acceptable use, Online Safety and Positive Behaviour policies must be followed at all times.

St Nicholas School does NOT give permission for pupils or parents/carers to take or publish video, photographic or screen shot images from the events of an online learning session (thus complying with the Data Protection Act 2018 and EU GDPR 2016).

All sessions will be recorded by the teacher (host) for safeguarding purposes. All recordings will be immediately uploaded to school's secure online cloud store. By having a true record of the events (accessible by the Senior Leadership Team), any potential complaints or incidents that may arise from an online lesson can be fully investigated. NB: All video lesson recordings will be deleted after period of 30 days or at the conclusion of an investigation (as appropriate).

Live-streamed Lessons – Privacy Notice

Before any Staff or Students engage in the (further) use of Live-streamed lessons or meetings please see to our Privacy Notice:

About Live-streamed lessons and the systems we use?

- What we use online lessons for?
  St Nicholas School uses secure online video conferencing platforms to communicate with parents and/or pupil groups, hold 'live' lessons via digital lessons, to record the achievement of learning and progress milestones and to share information, using the Earwig system. The information from progress milestones may also be shared with parents/carers by granting them viewing access to the records – consent will need to be given for this as there is the potential for group images to be included which could be seen by other families.

- How we use it in practice?
  Historically pupils have always been taught by staff to show learning and progress in school or community-based settings. This can now be applied to learning at home. Photographic evidence of this has historically been put into their workbooks. Currently, pupils are photographed and videoed engaging in lessons and this is then uploaded onto the secure Earwig system allowing parents/carers to potentially have access to images of their child and, potentially, their child's peers (if in a shared image).

- Do the live-streamed lesson companies need to gain permission from parents to photograph or video pupils?
  No, the companies are not holding a recorded copy of the images so they are not holding a permanent version of the images or events. St Nicholas School will record the session which will automatically be uploaded to the schools' online cloud storage system for safeguarding purposes and to have a record of the learning that has taken place to evidence progress. Still or video images would be then, potentially, shared across to our online and secure data system Earwig. After 30 days all recordings will be deleted permanently.

- Are the online accounts secure?
  The MS Teams and MS Skype for Business systems are fully encrypted. The Zoom system now is secure and encrypted with each session having a separate meeting ID and password, authorised participants only can be allowed access by the host (from a waiting room) and the meeting is locked so no late access can be given. Each school earwig account is a separate secure environment. Data is encrypted and each parent login must be approved by the school. Even then, each parent/carer can only see images which relate directly to their child.

- Does Earwig need to gain permission from parents to photograph or video pupils?
  As with any image based education tool, Child Protection is built in. The system is a Closed User Group – not available to those who have not been approved by the school and invited parents/carers. We have created an Earwig consent form that all parents/carers should complete. When the form has been completed if a parent/carer objects to their child participating externally in the Earwig process that child is flagged so that all records made for that child are automatically marked as 'Internal' and therefore not available to share with parents/carers. All

images/videos/documents remain the property of the school at all times.

- Do I need to give permission for my child to have their image used In internal records on the Earwig system?
No - Each school earwig account is a separate secure environment. Data is encrypted and each parent login must be approved by the school. Even then, each parent/carer can only see images which relate directly to their child.

- Do I need to give permission for my child to have their image used in accessible group records on the Earwig system?
Yes – if you wish to have access to records that may be of paired or group learning experiences then these images will need the permission from the families of all people involved.

If you would like to discuss anything in this privacy notice, please contact:
Stephen King (Deputy Head), Data Protection Lead – email: stephen.k@st-nicholas.kent.sch.uk

LINKS TO OTHER POLICIES

Online Safety/Child Protection/Data Protection
Acceptable Use of Technology
Staff Code of Conduct
Positive Behaviour Support
Acceptable Image Use
Anti-Bullying
Confidentiality
Lone Working
All curriculum Policies

STEPHEN KING
WRITTEN TERM 6 2020
RATIFIED BY CHAIRPERSONS ACTION 4 MAY 2021