Norwich Steiner School

Internet Safety Policy

Revised September 2019

Norwich Steiner School is committed to providing a safe learning environment for its pupils. This policy describes our curricular approach to information and communications technology (ICT) and online safety in the school. It reflects the school's ethos and curriculum, and so takes account of the age and developmental stage of pupils across the school. It forms part of our overarching safeguarding approach, This policy should be read alongside the school's mobile phone and electronic devices, anti-bullying, safeguarding and child protection and youth produced sexual imagery (sexting) policies and pupil internet safety agreement and curriculum policy.

Keeping Children safe in Education, DfE (Sept 2019) reminds us that:

'The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation- technology often provides the platform that facilitates harm.' and states that it '*is essential that children are safeguarded from potentially harmful and inappropriate online material*'.

Risk

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Although these risks are minimised in this school through our curricular approach to ICT, we realise that our pupils are at risk outside of school hours, so we work closely with parents to ensure that they have up to date information in order to help their children to stay safe.

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in a safe and appropriate way. The school takes every opportunity to help parents understand these issues through parents' evenings, talks from the Safer Schools Network, newsletters, regular e-safety bulletins, safeguarding input at parents evenings, information about national and local online safety campaigns etc. Parents are encouraged to support the school in promoting good online safety practice and to support their children in following school policies. **T**he DSLs act as a point of contact and source of information for parents.

Providing safeguarding information to pupils

We provide safeguarding information and guidance directly to the pupils across the school. Kindergarten and younger school pupils are provided with safety messages through specially designed developmentally appropriate narratives and the teachers address any issues or questions that these children may have in an age appropriate way. From class 5 pupils receive information and guidance via the PHSE curriculum, in sponsor and global issues lessons, including direct input from the Safer Schools Network, and teachers address any questions or issues as they arise.

Use of Technology in the school

Early Years (pupils aged 3-6)

No electronic devices or technology are used in the kindergarten. Children do not bring devices into school. There is therefore an extremely low risk of pupils accessing any harmful or illegal material online in school

Lower School (pupils aged 6-13)

No electronic devices or computers are used in lower school. Pupils are not permitted to bring personal electronic devices like ipads to school. Mobile phone use is not permitted in school at any time. Mobile phones brought to school as part of a back up system for safe travel are kept switched off in the pupil's bag. Pupils are closely monitored during break times. The risk of these pupils accessing harmful or illegal materials online whilst in school is therefore low.

Upper School (pupils aged 13-19)
Mobile phones are kept switched off and in pupils' bags, and may not be used on school premises without permission and supervision. Personal computers are generally not allowed in school, except for pupils in the last two years of their education. However pupils are unable to connect personal devices to the School internet, so the opportunity to access the Internet on their personal devices is limited to the possibility of their creating a local hotspot, using their mobile phone. Therefore, strict implementation of the School's 'no mobile phone use' policy and application of sanctions thereof, are critical in maintaining a safe environment.

Students have access to computers in Upper school in Class 8/9 to learn skills such as touch typing, but are not permitted at this age to use the internet. Pupils access the internet at school for the first time in class 9/10, when they are aged 14-16. Any pupil using a school computer is required to sign and abide by the school's pupil internet safety agreement before being given access to School computers.

Pupils in class 9/10 and 10/11 are only allowed internet access when supervised by a member of staff, and to undertake a specific task. At this stage pupils may use the school laptops for writing up assignments. Generic 'research' is generally not allowed and teachers take care to provide pupils with the literature they require for assignments to reduce the perceived need by pupils to carry out 'research'. Class 11/12 and 12/13 pupils (age 16-19) are allowed to use School computers to access the internet without close supervision.

The School has a system of signing laptops in and out, so that Browser histories and computer content can be monitored. The School computers also have software installed that allows a designated staff computer to carry out 'real time' monitoring of pupils use. The software is called NetSupport Assist for Schools and pupils are aware that at any time a member of staff may do a monitor check to see what pupils are looking at on their screens.

In practice, the school has found that checking computers at the end of the day and monitoring browser history allows the school support the pupils in learning to be safe on the internet. Pupils rarely shut computers down, and often leave open numerous pages on the internet browser. Any potentially inappropriate use is investigated and addressed, through safeguarding channels if needed.

The pupils are aware of this system and it is proving to be effective. We have considered the risks and benefits of monitoring versus blocking and filtering, mindful of our obligation to "*ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015) and believe that this approach is currently the most appropriate for safe and effective delivery of the curriculum for these older pupils. Feeling trusted in this way supports development of responsible and safe on-line behaviour. This approach also removes the perceived 'challenge' of a filter, and provides a method to continually, actively and realistically monitor, review and assess risks and safety, and so avoid complacency. Older students may need to research aspects of terrorism and counter-terrorism as part of their studies, and this approach enables staff to identify were such material is accessed for curriculum purposes.

The School continues to review this approach, taking into account statutory guidance and changes to risk, while remaining conscious that 'over-blocking', may adversely effect pupils' educational experience and ability to manage their online safety outside of school.

Staff Responsibilities
Staff acknowledge that children from kindergarten upwards will be accessing devices and content outside of school and are alert to any areas of concern which are addressed with parents or the safeguarding team as appropriate.

All staff have an awareness and understanding of online safety, including radicalisation, as part of wider safeguarding in the school, and this is reflected in safeguarding training. Upper school staff are alert to pupils' online activity in class and the DSLs act as a source of information for all staff. Training from the Safer Schools Network is provided for all staff, and the DSL, kindergarten manager and some teaching staff have also undertaken NSPCC training in keeping children safe online.The Lead DSP has also undertaken CEOP training, and is aware of the potential for serious child protection / safeguarding issues to arise from: sharing of personal data / images, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming. This includes the risk of radicalisation or being drawn into other criminal activities, as well cyberbullying, sexual harassment, peer on peer abuse, and child sexual exploitation and abuse.

Some Further information and Support

https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Organisation/Resource	What it does/provides
thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
the use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
lgfl	Advice and resources from the London Grid for Learning