Norwich Steiner School

Internet Safety Policy

Revised October 2021

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 policies and pupil internet safety agreement and curriculum policy.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers us to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

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

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g.consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school, sexually harass their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.

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. The 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 three years of their education. However, pupils are unable to connect personal devices to the school internet due to password protection, 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.

These pupils are assigned a school laptop. 13–15-year-old pupils may use these for writing up assignments. Generic research is not encouraged, 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, and a list of approved websites. Pupils aged 16-19 are allowed to use school laptops to access the internet without this close supervision.

In practice, we have found that checking computers at the end of the day and monitoring browser history allows us to 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 that children are safe from terrorist and extremist material when accessing the internet in school 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 where 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 affect pupils' educational experience and ability to manage their online safety outside of school.

Not all classrooms currently have Wi-Fi access, which is limited to staff areas, with intermittent signal in upper school classrooms, which teachers may boost if their lesson requires access. We will be upgrading the WIFI system, and will review our policy and procedures at the start of the spring term.

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 is provided annually 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 criminal activities, as well as cyberbullying, sexual harassment, peer on peer abuse, and child sexual exploitation and abuse.

Further information and Support

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- 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
- UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Support for Parents

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online