Norfolk House School

Online Safety Policy

October 2023

Contents

1. Aims

1.1. This is the Online Safety Policy of Norfolk House School (**School**).

1.2. The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which:

1.2.1. protects the whole School community from illegal, inappropriate and harmful content or contact;

1.2.2. educates the whole School community about their access to and use of technology;

1.2.3. establishes effective mechanisms to identify, intervene and escalate incidents where appropriate; and

1.2.4. promotes a culture of safety, equality and protection.

2. Scope and application

2.1. This policy applies to the whole School including the Early Years Foundation Stage (**EYFS**).

2.2. This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's technology whether on or off School premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

3. Regulatory framework

3.1. This policy has been prepared to meet the School's responsibilities under:

3.1.1. Education (Independent School Standards) Regulations 2014;

3.1.2. Statutory framework for the Early Years Foundation Stage (DfE, Sept 2022);

3.1.3. Education and Skills Act 2008;

3.1.4. Children Act 1989;

3.1.5. Childcare Act 2006;

3.1.6. Data Protection Act 2018 and UK General Data Protection Regulation (UK **GDPR**); and

3.1.7. Equality Act 2010.

3.2. This policy has regard to the following guidance and advice:

3.2.1. Keeping children safe in education (DfE, September 2023) (**KCSIE**);

3.2.2. Preventing and tackling bullying (DfE, July 2017);

3.2.3. Sharing nudes and semi-nudes: advice for education settings working with children and young people (DCMS and UKCIS, December 2020);

3.2.4. Revised Prevent duty guidance for England and Wales (Home Office, updated March 2023);

3.2.5. Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, February 2021);

3.2.6. Sexual violence and sexual harassment between children in schools and colleges (DfE, Sept 2021);

3.2.7. Searching, screening and confiscation: advice for schools (DfE, January 2018);

3.2.8. Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019);

3.2.9. Relationships Education, Relationships and Sex Education (**RSE**) and Health Education guidance (DfE, Sept 2021);

3.2.10. Teaching online safety in schools (DfE, June 2019); and

3.2.11. Harmful online challenges and online hoaxes (DfE, February 2021).

3.3. The following School policies, procedures and resource materials are relevant to this policy:

3.3.1. Pupil IT Acceptable Use Policy;

3.3.2. Staff IT Acceptable Use Policy;

3.3.3. Social Media Policy;

3.3.4. Safeguarding and Child Protection Policy;

3.3.5. Anti Bullying Policy;

3.3.6. Risk Assessment Policy for Pupil Welfare;

3.3.7. Staff Code of Conduct;

3.3.8. Whistleblowing Policy;

3.3.9. Data Protection Policy;

3.3.10. Mobile Device and Camera Policy;

3.3.11. School Rules; and

3.3.12. Relationships Education Policy.

4. Publication and availability

4.1. This policy is published on the School website and in the Virtual Staffroom.

4.2. This policy is available in hard copy on request.

5. Definitions

5.1. Where the following words or phrases are used in this policy:

5.2. References to the **Proprietor** are references to the Board of Directors of Norfolk House School Limited.

5.3. In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as technology).

6. Responsibility statement and allocation of tasks

6.1. The Proprietor has overall responsibility for all matters which are the subject of this policy.

6.2. The Proprietor is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Proprietor's response to this duty.

6.3. To ensure the efficient discharge of its responsibilities under this policy, the Proprietor has allocated the following tasks:

Task	Allocated to	When / frequency of review
Keeping the policy up to date and compliant with the law and best practice	Head of Pastoral Care	As required, and at least termly
Monitoring the implementation of the policy (including the record of incidents involving the use of technology and the logs of internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating effectiveness	" " "	As required, and at least termly
Online safety	" " "	
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the policy	" " "	As required, and at least annually
Formal annual review	Proprietor, Headmistress, Head of Pastoral Care	Annually

7. Role of staff and parents

Headmistress and Senior Leadership Team

7.1. The Headmistress has overall executive responsibility for the safety and welfare of members of the School community.

7.2. The Designated Safeguarding Lead is the senior member of staff from the School's leadership team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding and Child Protection Policy.

7.3. The Designated Safeguarding Lead will work with the School's ICT Consultant in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

7.4. The Designated Safeguarding Lead will regularly monitor the technology incident log maintained by the Head of ICT.

7.5. The Designated Safeguarding Lead will regularly update other members of the School's Senior Leadership Team on the operation of the School's safeguarding arrangements, including online safety practices.

School's ICT Consultant

7.6. The School's ICT Consultant advises upon and implements effective filtering systems so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

7.7. The School's ICT Consultant helps the School to implement systems which ensure that:

7.7.1. the School's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

7.7.2. the user may only use the School's technology if they are properly authenticated and authorised;

7.7.3. the School has effective filtering and monitoring systems in place and that they are applied and updated on a regular basis;

7.7.4. the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;

7.7.5. the use of the School's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation.

7.7.6. The School's ICT Consultant will report regularly to the Senior Leadership Team on the operation of the School's technology. If the School's ICT Consultant has concerns about the functionality, effectiveness, suitability or use of technology within the School, including of the monitoring and filtering systems in place, he will escalate those concerns promptly to the Designated Safeguarding Lead.

Head of ICT

7.8. The Head of ICT is responsible for maintaining the technology incident log (a central record of all serious incidents involving the use of technology) and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's safeguarding and child protection policy.

All staff

7.9. All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the School's policies and of safe practice with the pupils.

7.10. Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

7.11. Staff have a responsibility to report any concerns about a pupil's welfare and safety to the DSL and in accordance with this policy and the School's Safeguarding and Child Protection Policy.

Parents

7.12. The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. The School expects parents to promote safe practice when using technology and to:

7.13. support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

7.14. talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

7.15. encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

7.16. If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Lead (the Headmistress).

8. Access to the School's technology

8.1. Internet use is an important part of the school curriculum and is a necessary tool for pupils. It raises educational standards and helps to promote pupil achievement. Specifically, use of the internet allows for access to worldwide education resources and expert up-to-date resources for pupils.

8.2. The School provides internet access to pupils, and intranet, social media, and email access to staff, as well as other technology. Pupils and staff must comply with the respective acceptable use policy when using School technology. All such use is monitored by the School's ICT Consultant and Headmistress.

8.3. The School employs variety of methods aimed at ensuring that pupils and staff are unable to access inappropriate material:

8.3.1. DNSFilter: all internet requests pass through a DNS filter service which is enabled by the router. This screens the requests and helps block sites which may include content such as adult themes, gambling and violence.

8.3.2. ESET anti-virus software: is installed on all computers. It self-updates several times a day and its a regularly checked and maintained. Amongst other things, it helps to stop malware downloads to the computer and prevents inappropriate pop-up.

8.3.3. Google SafeSearch: computers in the ICT Suite are all protected by Google Safe Search, which is enabled via the DNS filter filter service (see above). It assists with preventing adult content from appearing on searches. A notice is also provided on-screen to alert pupils of incorrect usage, should it occur.

8.3.4. iPad settings: In the case of iPads, appropriate passcode-protected settings are used to limit the devices' functionality and the websites which can be accessed

8.3.5. Teaching of pupils: pupils are taught that they can only access the internet when supervised by an adult and should not make any changes to network settings to the computers in the ICT Suite or elsewhere in school. Similarly, they are taught that they are not permitted to install other software or programmes on the computers as this may affect the correct functioning of the network. It is explained to the pupils that their use of the network can be monitored by the network administrators. Pupils are encouraged to report any inappropriate use immediately to a member of the teaching staff, all of whom receive regular updated E-Safety Training.

8.4. The School's ICT Consultant receives and reviews a report of blocked webites on a weekly basis during term time and shares it with the School.

8.5. The Administrative Assistant checks the history of PCs and iPads used by children on a weekly basis during term time and maintains a log.

8.6. A log is maintained by teaching staff of which PC / iPad is used by which pupil, together with the date and time of its use.

8.7. Staff require individual user names and passwords to access the School's internet, intranet and social media sites and email system which must not be disclosed to any other person. Any member of staff who has a problem with their user names or passwords must report it to the Office Manager immediately.

8.8. No mobile electronic device (other than a staff laptop) may be connected to the School's network without the consent of the Headmistress. Where such consent is given, the use of any device connected to the School's network will be logged.

8.9. The School's Wi-Fi connection is not available for use by visitors to the School, unless the Headmistress gives her consent in a specific case. Its use will be logged in such a case.

9. Procedures for dealing with incidents of misuse

9.1. Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

Misuse by pupils

9.2. Anyone who has any concern about the misuse of technology by pupils should report it to the appropriate member of staff (referred to in the table below) so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the anti-bullying policy where there is an allegation of cyberbullying.

Type of misuse	Relevant policy	Reporting channel
Bullying	Anti-bullying	Head of Pastoral Care Note any incidents which give rise to safeguarding concerns must be referred on to the DSL
Sharing nudes and semi-nude images (sexting/youth produced sexual imagery)	Safeguarding and child protection policy [Sexual harassment/ peer on peer abuse policy (if separate)]	Head of Pastoral Care Who should then refer to the DSL who has overall responsibility for online safety matters
Harassment	Safeguarding and child protection policy [Sexual harassment/ peer on peer abuse policy (if separate)]	Head of Pastoral Care Who should then refer to the DSL who has overall responsibility for online safety matters
Upskirting	Safeguarding and child protection policy [Sexual harassment/ peer on peer abuse policy (if separate)]	Head of Pastoral Care Who should then refer to the DSL who has overall responsibility for online safety matters

Radicalisation	Safeguarding and child protection policy [Prevent Risk Assessment/ policy (if separate)]	Head of Pastoral Care Who should then refer to the DSL who has overall responsibility for online safety matters
Other breach of acceptable use policy	See relevant policy referred to in acceptable use policy	Head of Pastoral Care Who should then refer to the DSL who has overall responsibility for online safety matters

9.3. Anyone who has any concern about the welfare and safety of a pupil must report it to the DSL immediately in accordance with the School's child protection procedures (see the School's safeguarding and child protection policy).

Misuse by staff

9.4. Anyone who has any concern about the misuse of technology by staff should report it in accordance with the School's whistleblowing policy so that it can be dealt with in accordance with the staff disciplinary procedures.

9.5. If anyone has a safeguarding-related concern relating to staff misuse of technology, they should be report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's safeguarding and child protection policy.

Misuse by any user

9.6. Anyone who has a concern about the misuse of technology by any other user should report it immediately to the Designated Safeguarding Lead.

9.7. The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

9.8. If the School considers that any person is vulnerable to radicalisation the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

10. Education

10.1. The safe use of technology is integral to the School's curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices (see the School's curriculum policy).

10.2. As the safe use of technology is a focus in all areas of the curriculum, key safety messages are reinforced as part of assemblies and tutorial / pastoral activities and teaching pupils:

10.2.1. about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

10.2.2. to be critically aware of content they access online and guided to validate accuracy of information;

10.2.3. how to recognise suspicious, bullying or extremist behaviour;

10.2.4. the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

10.2.5. the consequences of negative online behaviour;

10.2.6. how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly; and

10.2.7. how to respond to harmful online challenges and hoaxes.

10.3. Those parts of the curriculum which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

10.4. The School's Pupil IT Acceptable Use Policy sets out the School rules about the use technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on a regular basis.

10.5. Technology is included in the educational programmes followed in the EYFS in the following ways:

10.5.1. children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

10.5.2. children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

10.5.3. children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

10.6. **Useful online safety resources for pupils**

http://www.thinkuknow.co.uk/

http://www.childnet.com/young-people

https://childnet.com/resources/smartie-the-penguin (EYFS)

https://www.childnet.com/resources/digiduck-stories (EYFS)

https://www.saferinternet.org.uk/advice-centre/young-people

https://www.disrespectnobody.co.uk/

http://www.safetynetkids.org.uk/

https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

https://www.bbc.com/ownit

https://www.gov.uk/government/publications/indecent-images-of-children-guidance-for-young-people/indecent-images-of-children-guidance-for-young-people

11. Training

Staff

11.1. The School provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.

11.2. Induction training for new staff includes training on the School's online safety strategy including this policy, the staff code of conduct, staff IT acceptable use policy and social media policy. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and or videos , cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes.

11.3. Where safeguarding incidents involve youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the School's policy on sharing nudes and semi-nude images and videos as set out in the behaviour and discipline policy and Searching, screening and confiscation: advice for schools (DfE, January 2018)

11.4. Staff also receive data protection training on induction and at regular intervals afterwards.

11.5. The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

Useful online safety resources for staff

http://swgfl.org.uk/products-services/esafety

https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

http://www.childnet.com/teachers-and-professionals

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

https://www.thinkuknow.co.uk/teachers/

http://educateagainsthate.com/

https://www.commonsense.org/education/

Cyberbullying: advice for Head teachers and school staff (DfE, November 2014)

Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)

Sharing nudes and semi-nudes: advice for education settings working with children and young people (DCMS and UKCIS, December 2020).

Online safety in schools and colleges: questions from the governing board (UKCIS, 2022)

Education for a connected world framework (UKCIS, 2020)

https://www.lgfl.net/online-safety/resource-centre

Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)

Myth vs Reality: PSHE toolkit (Childnet, April 2019)

SELMA Hack online hate toolkit (SWGFL, May 2019)

Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects (June 2019)

Harmful online challenges and online hoaxes (DfE, February 2021)

Professionals online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772.

NSPCC helpline for anyone worried about a child - 0808 800 5000

Internet Watch Foundation - internet hotline for the public and IT professionals to report potentially criminal online content

The Birmingham Children's Trust (local safeguarding partnership) has produced guidance on radicalisation which is available here: https://proceduresonline.com/trixcms1/media/3766/bct-csc-prevent-guidance-june-2018-181119.pdf

Parents

11.6. The school offers online workshops which deal with the safe use of technology, with particular emphasis on use of the internet and social media.

11.7. Parents are encouraged to read the acceptable use of technology by pupils policy for with their son / daughter to ensure that it is fully understood.

11.8. Useful online safety resources for parents

https://www.saferinternet.org.uk/advice-centre/parents-and-carers

http://www.childnet.com/parents-and-carers

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

https://www.thinkuknow.co.uk/parents/

http://parentinfo.org/

http://parentzone.org.uk/

https://www.net-aware.org.uk

https://www.internetmatters.org/

https://www.commonsensemedia.org/

Advice for parents and carers on cyberbullying (DfE, November 2014).

http://www.askaboutgames.com

https://www.ceop.police.uk/safety-centre

UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019)

LGfL: parents - scare or prepare

Thinkuknow: what to do if there's a viral scare online

12. Risk assessment

12.1. Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

12.2. The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

12.3. Headmistress has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

12.4. Day to day responsibility to carry out risk assessments under this policy will be delegated to Head of ICT who has been properly trained in, and tasked with, carrying out the particular assessment.

13. Record keeping

13.1. All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

13.2. All serious incidents involving the use of technology will be logged centrally in the technology incident log by the Head of ICT.

13.3. The information created in connection with this policy may contain personal data. The School's use of this personal data will be in accordance with data protection law. The School has published privacy notices on its website which explain how the School will use personal data.

14. Version control

Date of adoption of this policy	21.6.21
Date of last review of this policy	11.10.23
Date for next review of this policy	11.10.24
Policy owner (SLT)	Designated Safeguarding Lead
Policy owner (Proprietor)	Chair of Directors