Northbourne Park School (including EYFS)

E-Safety Policy

The policy applies to all staff

Date created: September 2014
Last Reviewed: September 2023
Date for review: September 2024
Owned by: Designated Safeguarding Lead
Reviewers: SMT
Approved by: Board of Governors

Introduction

The NPS E-Safety Policy is an integral part of our safeguarding provision and should be read in conjunction with the Safeguuarding and Child Protection Policy. It applies to all members of the school community (including staff, pupils, governors, volunteers, parents and carers, visitors and community users). It also applies to the use of personal digital technology. Its central purpose is to provide pupils, staff, parents and governors with a safe environment in which to use online technologies. The NPS E-Safety Policy is reviewed annually by the DSL, who is the Headmaster. The policy is overseen by the governing body and reflects related current legislation in the UK. The policy pays due regard to Keeping Children Safe in Education.

E-Safety is defined as Northbourne Park School's ability to:

- Protect and educate pupils, parents, governors and staff in their use of technology.
- Ensure that appropriate mechanisms to intervene and support any incident where appropriate.

The breadth of issues can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material.
- Contact: being subjected to harmful online interaction with other users.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce/Contract: Risks such as online gambling, fraud, blackmail, hacking, trafficking, persuasion or inappropriate advertising, phishing and or financial scams.

The School has a duty to provide:

- Appropriate e-Safety training for all staff that is relevant and regularly up to date.
- Online safety training and information for Governors as part of their safeguarding training
- Support mechanisms for pupils and staff facing online safety issues.
- e-Education and support for parents and the whole school community.
- Clear, understood and respected online safety e-safety policies and acceptable use policies.

The School will make clear to all pupils:

- Where to go for help, if they feel uncomfortable about anything they see.
- Where to go for help if anybody online asks them for their personal details such as their address.
- Who to tell, if anybody sends them hurtful messages on the internet or mobile phones.
- What the acceptable rules are at Northbourne Park for using the internet.
- What sanctions are in place to enforce these acceptable rules.
- What the risks are of posting inappropriate content on the internet.

All staff know:

- What is meant by the term cyber-bullying and the effect it can have on themselves and pupils.
- Clear reporting mechanisms with a set of actions are in place for staff or pupils who feel that they are being bullied online.

Scope of the Policy

This policy applies to all members of Northbourne Park School (including staff, pupils, volunteers, parents, guardians, carers, visitors and community users) who have access to and are users of the school's ICT systems, whether the users are on of off school grounds.

The NPS e-Safety Policy relates to other published school policies and in particular the following:

NPS ICT Policy
NPS Anti- Bullying Policy
NPS Child Protection Policy
NPS Staff Disciplinary Procedure
NPS Form Tutor Role
NPS Professional Standards for Teacher
NPS Staff Safe Working Practices with Children
NPS Boarding Staff Handbook
NPS Data Protection Policy

NPS Health and Safety Policy Statement
NPS Confidentiality Policy
NPS Anti-Cyberbullying Policy
NPS Photographic Images Policy
NPS Visitors Policy
NPS Pre-Prep Mobile Phone and Camera Policy
NPS GDPR Policy

The school is registered under and subject to the current Data Protection Act with the I.C.O.

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors

The Education and Inspections Act 2006 empowers Heads, to such extent as is reasonable, to regulate the behaviour of pupils when they are on or off the school site. It empowers members of staff to impose disciplinary penalties for inappropriate behaviour. Incidents of cyber-bullying, or other e-Safety incidents covered by this policy, might take place outside of the school, but are nonetheless linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the NPS Discipline Policy (Prep) and the NPS Discipline Policy (Pre-Prep).

The school will deal with E-Safety incidents and other associated behaviour, informing parents or guardians accordingly.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the NPS E-Safety Policy and for reviewing its effectiveness. Governors will:

- Hold regular meetings with the DSL
- Receive reports of online safety incidents

- Check provision of online safety
- Review online safety at committee meetings
- Ensure that the filtering and monitoring provision is reviewed and recorded at least annually

The Designated Safeguarding Lead (DSL)

The DSL, who is the headmaster, takes lead responsibility for online safety and has a duty of care for ensuring the safety of all members of the Northbourne Park community. The DSL oversees the effective implementation of this policy through the NPS Health and Safety Committee and is trained in E-Safety issues, aware of the potential for serious child protection and safeguarding issues relating to the sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

The DSL is responsible for ensuring that other relevant staff, including the ICT Manager, receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.

The DSL will ensure that there is a system in place to allow for supporting those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headmaster and (at least) one other member of the Senior Management Team are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

ICT Manager

The school's ICT Manager supports the work of the DSL and whose work falls under the jurisdiction of the NPS Health and Safety Committee, which meets termly, chaired by the Bursar. E-Safety will appear as an agenda item for all meetings and the ICT Manager will attend every meeting to brief the committee. The ICT Manager liaises regularly with the DSL.

The ICT Manager's role is to:

- Attend all Health and Safety Committee meetings.
- Monitor day-to-day e-safety issues and inform the DSL, who holds overall responsibility for e-safety.
- Support the DSL in the effective review and implementation of the NPS E-Safety Policy.
- Inform all staff of the procedures in the event of an e-safety incident.
- Source training and advice for staff.
- Receive reports of e-safety incidents.
- Create a log of incidents to inform future e-safety developments.
- Ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensure that the school meets required e-Safety technical requirements and any Local Authority / other relevant body e-Safety Policy / Guidance that may apply.
- Ensure that all users of the school ICT network can only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- Check that the filtering policy is applied and updated on a regular basis, and that the school is compliant with Keeping Children Safe in Education and DfE Guidance (2022): Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
- Keep up to date with e-Safety developments and inform other staff as required.
- Monitor use of the internet, any VLEs, remote access, Wi-Fi, email and report any misuse to the DSL.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that they:

- Have an up to date awareness of e-safety matters and of the NPS E-Safety Policy.
- Have read, understood and signed the NPS Staff Acceptable Use Policy / Agreement (AUP)
- Report any suspected misuse or problem to the DSL for investigation.
- Ensure that all digital communications with pupils and parents should be on a professional level and only carried out using official school systems.
- Embed e-Safety issues into all aspects of the ICT curriculum and the PSHE programme.
- Instruct pupils to follow the NPS E-Safety Policy and NPS ICT Code of Conduct.
- Provide pupils with a good understanding of research skills, the need to avoid plagiarism and uphold copyright regulations.
- Monitor the use of digital technologies, mobile devices, cameras and other electronic devices in school hours.
- Implement current policy with regard to these devices, including boarding time.
- Help staff to locate safe internet sites suitable for their use.
- Help staff to understand the processes in place for dealing with any unsuitable material found in internet searches.

Pupils

Pupils are responsible for:

- Using the NPS technology systems in accordance with the ICT Code of Conduct Policy.
- Using effective research skills, whilst upholding copyright regulations and without the need to plagiarise.
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials.
- Knowing and understanding policies on the use of mobile devices and digital cameras.
- Knowing and understanding policies on the taking / use of images and on cyber-bullying.
- Understanding the importance of adopting good e-safety practice when using digital technologies out of school.
- Recognising that the NPS E-Safety Policy in some instances which relate to the school, covers their online life out of school

Parents and Guardians

Parents and Guardians play a vital role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. NPS takes every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local e-Safety campaigns and literature.

Parents and Guardians are encouraged to support NPS in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website.
- their children's personal devices in the school (where this is allowed).
- websites and Social networking sites outside of the School network.

We share information with parents/carers about:

- what systems we have in place to filter and monitor online use.
- what we are asking children to do online, including the sites they will be asked to access.
- who from the school (if anyone) their child is going to be interacting with online.

Community Users

Community Users who access school systems and IT services as part of the wider NPS provision will sign the NPS Community User Acceptable Use Agreement before being provided with access to school systems.

Teaching and learning

The Internet and digital communications are essential educational tools. The school recognizes its duty to provide pupils with high-quality Internet access as part of their learning. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school is committed to teaching children how to use the internet safely.

The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils. Teachers will teach all pupils at the beginning of every academic year what Internet use is acceptable and what is not and give clear objectives for Internet use. Staff will also teach all pupils in the Prep School the effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation. Through the course of the ICT curriculum, staff will teach all Prep School pupils the importance of cross-checking information before accepting its accuracy and not breaching copyright laws.

Teachers will teach all Pupils how to report inappropriate Internet content and will teach all Pupils to inform members of staff if they are aware of any face-to-face or remote contact with people outside the school.

The Four C's

In line with KCSIE 2023, each student within our school is taught the Four C's, namely – Content, Contact, Conduct and Commerce/Contract. It is the School's responsibility to educate the children on how to adhere to this protocol, why it is important and the benefits of staying as safe as possible at all times when online.

The Four C's are broken down into the following definitions:

Content:

Being exposed to illegal, inappropriate or harmful content (for example: pornography, fake news, racist, misogynistic, self-harm, suicide, anti-Semitic, radical 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 for purposes of grooming)

Conduct:

Personal online behaviour that increases the likelihood or, or causes, harm (for example, making, sending and receiving explicit images, sharing others' explicit images and online bullying, future references etc)

Commerce/Contract

Risks such as online gambling, fraud, blackmail, hacking, trafficking, persuasion or inappropriate advertising, phishing and or financial scams. If any of the pupils, visitors or staff are at risk at Northbourne Park School, this should be reported to the Anti-Phishing Working Group (https://apwg.org/)

This initiative is to be taught across the School, in ICT lessons and assemblies, at the appropriate level for each form, and all refreshed termly under the catch phrase of 'The Four C's'

E-mail

Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive any offensive e-mail. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated cautiously and attachments treated as suspicious and not opened even if the author is known, unless being supervised or in lesson where advice can be sought. The sending or forwarding of chain letters is not permitted. The sending or forwarding of unproductive or nuisance emails is not permitted.

Published content and the school web site

Staff or pupil personal contact information will not be published. The contact details given online will be with the school office only. The Headmaster will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Group photographs rather than full-face photos of individual children will be used in preference. Full names of pupils will not be used anywhere on the school Website or other on-line space, in association with photographs without prior consent.

Written permission from parents or guardians is required before photographs of pupils are published on the school Website or online. We will only publish work with the permission of the pupil and parents/guardians. Pupil image file names will not refer to the pupil by name.

Parents will be clearly informed by the DSL of the school policy on image-taking and publishing, both on school and independent electronic devices.

Social networking and personal publishing

The school does not allow access to social networking sites, and will educate pupils in their safe use at home. Newsgroups will be blocked unless a specific use is approved. The school advises pupils never to give out personal details of any kind which may identify them, their friends or their location.

We advise pupils and parents that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Pupils are advised to use nicknames or avatars when using social networking sites at home.

Pupils are advised not to arrange to meet strangers unless accompanied by a known adult, whether the stranger is a child or an adult. Never discuss or divulge personal "log in" passwords or allow anyone to use your area.

Managing filtering

Appropriate Filtering and Monitoring

Governors liaise with school leaders to ensure that all relevant staff have an awareness and understanding of the filtering systems in place and that they are managed effectively. Methods to identify, assess and minimise risks, including filtering and monitoring, will be reviewed annually.

Governance will ensure that the school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies will consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

Northbourne Park School will do all we reasonably can to limit children's exposure to online risks through the school provided IT systems and will ensure that appropriate filtering and monitoring systems are in place, without 'over-blocking'. All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation. Filtering breaches or concerns identified through our monitoring approaches will be recorded and reported to the DSL who will respond as appropriate.

Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the Internet Watch Foundation and the police. When implementing appropriate filtering and monitoring, Northbourne Park School will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Filtering and monitoring is carried out by Securus, Dimension, Google Safe Search and Watchguard. Any breaches result in an automated email that is sent to the Head of IT who reports regularly to the DSL, who then decides what actions need to be taken. The effectiveness of the filter and monitoring software is tested as part of governance reviews annually.

Day pupils are not allowed mobile or smartphone technology in school. Boarders have restricted access and are monitored by boarding staff during phone time.

Northbourne Park School acknowledges that whilst filtering and monitoring is an important part of school online safety responsibilities, it is only one part of our approach to online safety.

Learners will use appropriate search tools, apps and online resources as identified following an informed risk assessment. Learners internet use will be supervised by staff according to their age and ability. Learners will be directed to use age appropriate online resources and tools by staff.

If staff or pupils come across unsuitable on-line materials, the site will be reported to the ICT Manager, who will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Smart Watches and Future Technology

Due to the 'tech nature' and ever changing world with which we all now live, children owning smart watches is on the increase. As a school, we have the educational responsibility to ensure that we implement the correct amount of supervision, guidance and control over the use of smart watches when at school. If the smart watch is able to connect to the internet as a standalone device, then they are not permitted at NPS.

Like in all of the IT measures and policies Northbourne Park School has in place, boarders with smart watches must abide by the same protocols put in place for the use of mobile phones. Day pupils are not permitted to use their smart watches in conjunction with a mobile phone or the School Wifi at any stage. Any misuse of these devices will carry a confiscation in line with the rest of the School's ICT Code of Conduct.

Please refer to the school's Safeguarding and Child Protection Policy for responding to cases of Sexting, Online Child Sexual Abuse and Exploitation, Indecent Images, Cyber-bullying and Radicalisation

Authorising Internet access

All staff will read and sign the *NPS Staff Acceptable Use Policy / Agreement (AUP)* before using any school ICT resource. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems. At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

The ICT Manager will ask parents to sign and return a consent form for their child.

Any person not directly employed by the school will be asked to sign an "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

The ICT Manager will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective. A risk assessment will be carried out for any new technology introduced to the school.

Liaising with parents and handling e-Safety complaints

The school is aware of the need to communicate regularly with parents, carers and guardians about the importance of children being safe online outside of school. Parents have access to the school's E-Safety Policy on the school website and are informed that children will be provided with supervised access to the internet.

Complaints of Internet misuse will be dealt with by a member of the SMT. Complaints concerning Child protection must be dealt with in accordance with the school's Safeguarding and Child Protection policy. The staff will inform pupils and parents of the consequences for pupils misusing the Internet.

Sanctions

Any pupil caught misusing the School's ICT facilities, whether reported by a child, member of staff; parent or indeed the School ICT Security programmes shall be fully investigated. If found to be in breach of the School's policy, sanctions will be issued in line with the school's Discipline Policy.

Introducing the e-Safety policy to pupils

The ICT Manager will post e-Safety rules in all rooms where computers are used and remind pupils of them regularly. The System Administrator will remind pupils that network and Internet use will be monitored and appropriately followed up. The Teachers will embed e-Safety training within the ICT scheme of work or the Personal Social and Health Education (PSHEE) curriculum.

Staff and the e-Safety policy

All staff will have access to the School e-Safety Policy and the DSL will provide regular reminders to staff. Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.

Bring Your Own Device Policy (BYOD)

All staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. Pupils are not permitted to use mobile phones during the school day. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden, and will be investigated. All staff will monitor the use by pupils of mobile phone cameras and keeps this practice under review.

Games machines including the Sony Playstation, Microsoft Xbox and others which have Internet access which may not include filtering are not permitted to be used at the school at any time.

Staff at NPS are allowed to bring in devices and use the NPS network to access the internet provided they put in the security settings and do not affect the operation of equipment already on the network. If device filtering is imposed as a security measure then the members of staff would have to register the device with the ICT Manager. The school accepts no responsibility for any loss or damage caused by any physical intervention or error in data transaction. Pupils with SEND are permitted to bring in their own laptops with the permission of the SENCo, and under the supervision of staff.

Only pupils that are classed as full boarders are allowed to use mobile devices on the school premises unless prior arrangement is made for an exception. Mobile devices are issued at the discretion of the boarding staff. The devices are required to be registered with the ICT manager if the Pupil wishes to use the school's filtered internet system. The ICT manager will put any settings in required for connection. The school accepts no responsibility to ensure compatibility between its network and with any mobile device. Types of devices will be accessed for security applications and access maybe refused.

The school has the right to withdraw any mobile device or its network connection.

If a Pupil wishes to use an unfiltered alternative method of receiving an Internet connection then they must bring this to the attention of a member of staff and be supervised. It is accepted that at the present time the IT department can not filter or monitor such connections.

The school's policies about digital and video images still apply and images should not be taken of a pupil or member of staff, without prior consent.