Northbourne Park School
e-Safety Policy

Author	Issue date	Review Period	Last Review date	Purpose	Scope	Version	Agreed by
DOPECA / ICT	Nov 2014	ANNUAL	Nov 2014	Safeguarding	All pupils, staff, governors, parents	1	HM
”	”	”	June 2015	”	”	2	EDUCATION COMMITTEE
DOPECA /ICT	Nov 2014	BI ANNUAL	Sept 2016	Safeguarding	All pupils, staff, governors, parents	3	DOPECA/ICT
SR/CS	Sept 2018	BI ANNUAL	Sept 2020	Safeguarding	All pupils, staff, governors, parents	3	HM
SR/CS	Sept 2020	Annual	Sept 2021	Safeguarding	All pupils, staff, governors, parents	3	HM

Contents

Northbourne Park School
e-Safety Policy

Bring Your Own Device Policy
Managing emerging technologies
Local Policy

Introduction

The *NPS e-Safety Policy* is an integral part of our safeguarding provision. Its central purpose is to provide pupils, staff, parents and governors with a safe environment in which to use new technologies. The *NPS e-Safety Policy* is reviewed annually by the Director of Pastoral and Extra-Curricular Activities, the ICT Coordinator and is overseen by the Headmaster.

It reflects related current legislation in the UK.

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

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

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

1. **Content**: being exposed to illegal, inappropriate or harmful material.
2. **Contact**: being subjected to harmful online interaction with other users.
3. **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm.

The School has a duty to provide:

- Appropriate e-Safety training for all staff that is relevant and regularly up to date.
- 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

Northbourne Park School
e-Safety 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 *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, or a nominated sub-committee are responsible for the approval of the *NPS e-Safety Policy* and for reviewing its effectiveness.

Headmaster and Senior Management

The Headmaster has a duty of care for ensuring the safety (including the e-Safety) of all members of the Northbourne Park community.

The Headmaster is responsible for ensuring that the e-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.

The Headmaster will ensure that there is a system in place to allow for monitoring and support of 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.

Northbourne Park School
e-Safety Policy

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

Child Protection Officer

The Headmaster together with the Bursar, oversee the effective implementation of this policy through the *NPS Health and Safety Committee*.

The Headmaster (Mr Sebastian Rees) is also the school's current *Designated Child Protection Officer*. The Child Protection Officer is trained in e-Safety issues and 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.

E-Safety Officer

***The e-Safety Officer* is Shaun Carlton,** who is ICT Manager. NPS is a small prep school and the e-safety officer's role 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 e-Safety officer will attend every meeting to brief the committee.

The e-Safety Officer's role is

1. Attend all Health and Safety Committee meetings.
2. Manage day-to-day responsibility for e-safety issues.
3. Lead in the effective review of the *NPS e-Safety Policy*.
4. Inform all staff of the procedures in the event of an e-safety incident.
5. Source training and advice for staff.
6. Liaise with the Local Authorities and with school technical staff.
7. Receive reports of e-safety incidents.
8. Create a log of incidents to inform future e-safety developments.

System Administrator

The System administrator is normally the IT Manager, whose responsibilities are as follows:

- 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.
- 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 Headmaster.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that they:

1. Have an up to date awareness of e-safety matters and of the *NPS e-Safety Ppolicy.*
2. Have read, understood and signed the *NPS Staff Acceptable Use Policy / Agreement (AUP)*
3. Report any suspected misuse or problem to the Headmaster or IT Manager for investigation.
4. Ensure that all digital communications with pupils and parents should be on a professional level and only carried out using official school systems.
5. Embed e-Safety issues into all aspects of the ICT curriculum and the PSHE programme.
6. Instruct pupils to follow the *NPS e-Safety Acceptable Use Policy* and *NPS ICT Code of Conduct.*
7. Provide pupils with a good understanding of research skills, the need to avoid plagiarism and uphold copyright regulations.
8. Monitor the use of digital technologies, mobile devices, cameras and other electronic devices in school hours.
9. Implement current policy with regard to these devices, including boarding time.
10. Help staff to locate safe internet sites suitable for their use.
11. 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.

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 Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.

The System Administrator and teachers will teach all pupils in the Prep School at the beginning of every academic year what Internet use is acceptable and what is not and give clear objectives for Internet use.

The ICT 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.

The ICT staff, through the course of the ICT curriculum, will teach all Prep School pupils the importance of cross-checking information before accepting its accuracy and not breaching copyright laws.

The ICT staff will teach all Pupils how to report inappropriate Internet content.

The ICT staff 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.

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.

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 System Administrator of the school policy on image-taking and publishing, both on school and independent electronic repositories.

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.

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

If staff or pupils come across unsuitable on-line materials, the site will be reported to the System Administrator.

The System Administrator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Responding to cases of Sexting, Online Child Sexual Abuse and Exploitation, Indecent Images, Cyber-bullying and Radicalisation

The following guidance and information, highlights Northbourne Park School's procedures regarding common online safety concerns including sexting, online child sexual abuse and exploitation, indecent images, cyber-bullying and radicalisation:

Sexting

NPS ensure that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating incident images of children (known as "sexting").
The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

NPS views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the ***Designated Child Protection Officer*, (Mr Sebastian Rees - Headmaster)** who in turn will seek advice from the LADO and /or Kent Police.

Online Child Sex Abuse

Northbourne Park School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming, as well as the consequences and possible approaches which may be employed by offenders to target children and how to respond to concerns.

The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

NPS views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the – ***Designated Child Protection Officer*** **(Mr Sebastian Rees - Headmaster)**.

If the school is unclear if a criminal offence has been committed then the ***Designated Child Protection Officer*** **(Mr Sebastian Rees - Headmaster)** will obtain advice immediately through the LADO and/or Kent Police.

Indecent Images

Northbourne Park School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

If the school is unclear if a criminal offence has been committed then the ***Designated Child Protection Officer*** **(Mr Sebastian Rees –Headmaster)** will obtain advice immediately through the LADO and/or Kent Police.

Cyber-bullying

Cyberbullying, along with all other forms of bullying, of any member of Northbourne Park School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

All incidents of online bullying reported will be recorded.

There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

If the school is unclear if a criminal offence has been committed then the ***Designated Child Protection Officer*** **(Mr Sebastian Rees - Headmaster)** will obtain advice immediately through the LADO and/or Kent Police.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber-bullying and the schools e-Safety ethos.

Radicalisation

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.

When concerns are noted by staff that a child may be at risk of radicalisation online then the ***Designated Child Protection Officer*** **(Mr Sebastian Rees – Headmaster)** will be informed and they are to seek advice immediately through the LADO and/or Kent Police.

Policy Decisions

Authorising Internet access

All staff will read and sign the "Staff Code of Conduct for ICT" 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 System Administrator 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 System Administrator 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.

Handling e-Safety complaints

Complaints of Internet misuse will be dealt with by a member of the SMT.

Any complaint about staff misuse must be referred to the Headmaster using the Notifiable Incidents Form.

Complaints concerning Child protection must be dealt with in accordance with the school child protection policy.

The System Administrator will inform pupils and parents of the consequences for pupils misusing the Internet.

Sanctions

Pupils

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 then a sanction of no ICT access for a period of two weeks shall be enforced. Limited access will be provided by the IT Manager for lesson time and prep. This to be allocated on an automated timing system set by the IT Manager. The parents/guardians of the child to be informed and a record of the incident is kept. A second offence will result in the same sanction, including a formal meeting with child, Headmaster and parents/guardian, with a record of the meeting to be kept. More intensive monitoring of the individual pupil and their access to the internet and ICT facilities is then kept for a period of a month.

Staff

All incidences are to be fully investigated by the Headmaster in conjunction with the IT Manager. A meeting with the individual teacher to be held with a record kept. Further sanctions are to be decided by the Headmaster in consideration with the severity of the report. This may include formal warnings, written or verbal, to enhanced monitoring and screening of the individual's ICT usage.

Communications Policy

Introducing the e-Safety policy to pupils

The System Administrator 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 System Administrator will provide regular reminders to staff. Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.

The System Administrator will manage filtering systems and monitoring ICT use will be supervised by Senior Management, who will ensure clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting Parents' and Guardians' support

Parents' and Guardians' attention will be drawn to the School e-Safety Policy in newsletters, the Parents' Handbook and on the school Web site.

The System Administrator will maintain a list of e-safety resources for parents/guardians.

The System Administrator will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

Bring Your Own Device Policy (BYOD)

Managing emerging technologies

We will examine emerging technologies against educational benefit and a risk assessment will be carried out before use of them in school is allowed.

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.

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD

that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

Local Policy

The standard policy of ICT code of conduct and aforementioned policy statements apply with the following amendments and additions. These will be subject to periodic review.

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 System Administrator. The school accepts no responsibility for any loss or damage caused by any physical intervention or error in data transaction.

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 System Administrator if the Pupil wishes to use the school's filtered internet system. The System Administrator 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. Present policy is that Microsoft based products provide a higher risk than Apple, Android, Kindle or Nintendo Products and are therefore not allowed. This will be reviewed and may change.

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.

Special e-Safety consideration should be given to the use of mobile devices incorporating cameras, in bedrooms and near shower or bathroom areas.

Pupils should also be warned about contacting strangers and arranging to meet them, without an adult present.

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.