PHOENIX PRIMARY SCHOOL

Online Policy and procedures, including Use of Images and Cyber-Bullying

National Online Safety®

Date written:	September 2020
Date received by staff:	September 2020 (updated 2023)
Date agreed by Local Governing Body:	September 2023
Date to be reviewed:	September 2024

Contents

1. Aims and Overview

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Local Governing Body (LGB)

The LGB has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The LGB will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).
All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.
The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the SLT, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers
All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents
Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4.1 Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.
In **EYFS** and **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

4.2 Why Safe Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

4.3 Internet use will enhance learning

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

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4.4 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. They will also be taught as young as possible how to manage and to be aware of their digital footprint.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and virtual learning environment (VLE). This policy will also be shared with parents.
Online safety will also be covered during parents' evenings.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6.0 Cyber-bullying
6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also our behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their groups, and the issue will be addressed in assemblies.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHCE) education, and other subjects where appropriate.
All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Peer on Peer abuse

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or

Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7.Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

7.1 Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies will be discussed with LEA/EIS.

7.2 E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

7.3 Published content and the school Website

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The ICT Subject Leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

8. Use of Images

8.1 Publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site (see below for more details).

Pupil's work can only be published with the permission of the pupil and parents.

Photographs and video for school and family use are a source of innocent pleasure and pride, which can enhance the self-esteem of children, young people and their families. Parents/carers are not required to comply with the Data Protection Act 1998 when taking photographs for their own private use of their children at an organised event. Parents should not be stopped from taking photographs for their own private use because of concerns of contravening the Data Protection Act.

However, we must always be mindful of the need to safeguard the welfare of children in our school, and issues of child protection, data protection and parental consent will be given careful thought. Images may be used to harm children, for example as a preliminary to 'grooming' or by displaying them inappropriately on the Internet.

This policy will apply to all forms of publications, print, film, video, DVD, on websites and in the professional media.

Where another body provides services or activities separately, using the school premises, the Governing Body will ensure that the body concerned has appropriate policies and procedures in place regarding safeguarding children.

8.2 Consent forms

- All parents of pupils in the school will be asked to sign a consent form to gain permission to publish photographs in public places (including websites)
- If parents/carers disagree over consent for their child, it will be treated as if consent has not been given.
- All adults in the school will be asked to sign a consent form to gain permission to publish photographs in public places (Including websites)

8.3 Parents and carers and use of images

- The school will decide if the event is one at which photography and videoing will be permitted.
- When informing parents of the event, they will be informed of the school's decision.

- If general shots are to take place such as at a school fete, visitors will be informed in the invitation, so that general consent is implied by attendance.
- Only images of children suitably dressed will be allowed to reduce the risk of images being used inappropriately. Special consideration will be given to photographs taken during PE (sports day) and swimming.
- Those parents and carers in the school to help with assisting children to dress or change will not be allowed to take photos or videos during this time.
- If a photograph is likely to be used again it will be stored securely and only accessed by those people authorised to do so. We will not re-use photos more than one year old unless they do not contain people.
- When photos are destroyed, the negatives will be destroyed as well, where the image is kept electronically (e.g. CD the disk will be made unusable)

8.4 Online, images and the curriculum
All children have undertaken workshops to understand the need for safety using electronic devices and to how to protect themselves. All images captured in lessons are to be stored safely on the school's system and not to be transmitted to any external devices.

9. Use of mobile technology
Pupils are not to bring mobile devices into school, only at the express wish of parents on the grounds of safety to and from school.
If such agreement is agreed with the school, the child is to hand in their phones to Reception upon arrival where they will be recorded and stored in a safe, they can pick them up at the end of school.

If a mobile device is brought in and seen by a member of staff it will be taken away and stored safely in the safe, staff will then inform parents.

10.0 Staff using work devices

10.1 Outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
If staff have any concerns over the security of their device, they must seek advice from the ICT manager.
Work devices must be used solely for work activities.

10.2 Inside School
Information stored within the school will be stored securely on school servers in line with LA and Kent guidelines. Security of data stored overseen by service provider and at present NO CLOUD STORAGE WILL BE CONSIDERED. Movement of data will take place only via encrypted pen drives or by the USO effect system to ensure secure passing of data. No data shall be emailed via unsecure providers. All laptops and mobile devices will be password protected.

10.3 Social networking and personal publishing
The school/ MGFL will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind, which may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

10.4 Managing filtering
The school will work with LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

10.5 Managing video conferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

10.6 Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Staff will be issued with a school phone where contact with pupils/parents is required.

10.7 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

10.8 Mobile Phone/Online Safety (EYFS)

All school owned devices will be used in accordance with the school's Staff Technology Acceptable Use Agreement and with appropriate safety and security measures in place. Staff and pupils in Key Stage 1 and 2 will be given personal usernames and passwords to use on laptops and iPads. Staff will supervise EYFS children at all times.

Staff should be particularly aware of the professional risks associated with the use of electronic communication (e-mail; mobile phones; texting; social network sites) and should familiarise themselves with advice and professional expectations outlined in the school's Online Safety Policy and is also reflected in the EYFS policy.

Phoenix Primary School recognises the specific risks that can be posed by mobile phones and cameras and in accordance with KCSIE and has appropriate policies in place that are shared and understood by all members of the school community. Further information reading the specific approaches relating to this can be found in the school's Online Safety Policy and is also reflected in the EYFS policy.

Filtering and monitoring is an important part of school's online safety responsibilities, it is only one part of our approach to online safety. Pupils and adults may have access to systems external to the school control such as mobile phones and other internet enabled devices and technology and where concerns are identified appropriate action will be taken

Phoenix Primary School recognises that many pupils and parents will have unlimited and unrestricted access to the internet via 3G and 4G in particular this is external to the school's control such as mobile phones and other internet enabled devices. Where concerns are identified appropriate action will be taken.

Personal mobile phones, cameras and video recording equipment cannot be used when in the presence of children on school premises including the swimming pool. Whether this be on site or a public pool is used.

In EYFS, all mobile phones must be stored securely (locked away) out of reach within the setting during contact time with children. (This includes staff, visitors, parents, volunteers and students).

Childminders must comply with the same guidelines as for parents.

In the case of school productions and sports day, parents/carers are permitted to take photographs/video footage of their own child in accordance with school protocols but we strongly advise against the publication of any such photographs on social networking sites. Most Pre-Prep events will be videoed / photographed by school staff and then made available to parents.

Personal mobiles, cameras or video recorders should not be used to record classroom activities, School equipment only should be used

All telephone contact with Parents/Carers should be made on the school telephone

All parents will be asked for permission for the school to photograph their children upon the child's entry to the school. Permission can be rescinded at any time, by the parent or carer in writing.

All Staff are expected to have read and understood this policy and will abide by this policy statement and know which other policies it should be cross-referenced with.

11 How the school will respond to issues of misuse

Where a pupil misuses the school's ICT system or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT system or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. CCTV Use within school

CCTV is used within school for the safety and security of staff and pupils, as well as safeguarding the premises. Visitors and members of the school will be made aware of the CCTV used within the school and it will be screened appropriately.

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

14.Policy Decisions

Authorising Internet access

All staff must read and sign the Online-Safety agreement before using any school ICT resource.

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

Parents will be asked to sign and return a consent form.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor LEA can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

Age Related Access

Students will be taught age related games, videos and clips. When made aware of students accessing inappropriate materials parents will be informed, which may lead to further authorities being involved.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Parents and pupils will need to work in partnership with staff to resolve issues.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to Online-safety.

15.Communication of the Policy and Procedures

Introducing the Online policy to pupils

Online rules will be posted in all networked rooms with Internet access and discussed with the pupils at the start of each year.

Pupils will be informed that network and Internet use will be monitored.

Staff and the Online policy

All staff will be given the School Online-Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff training in safe and responsible Internet use and on the school Online-safety Policy will be provided as required.

Enlisting parents' support

Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site.

Internet issues will be handled sensitively, and parents will be advised accordingly.

Staff Responsibilities

Personal mobile phones/devices are to be used in designated staff areas only.

Use of social media sites is to be for personal use only. Any staff, students or reference to School life placed upon such sites may be construed as bringing the School into disrepute.

Personal data is to remain securely on school premises.

Photographs or videos of children are to be curriculum related and be taken on school equipment.

Signed by staff:

Date: