PORG International School

e-Safety Policy

Prepared by:	Barbora Gazdova, Jaroslav Filip	Date: September 2023
Last update by:	Barbora Gazdova	Date: September 2026
Approved by:	Dagmar Dluhosova	

Content

INTRODUCTION 3

PURPOSE 3

AIM 3

THE FOUR AREAS OF ONLINE RISK 4

DIGITAL TECHNOLOGY 4

ELECTRONIC COMMUNICATION 4

WORLD WIDE WEB 4
EMAIL 4
SOCIAL NETWORKING 5
VIDEO CONFERENCING 5
MANAGING EMERGING TECHNOLOGIES 6
PUBLISHED CONTENT AND THE SCHOOL WEBSITE 6
PUBLISHING PUPILS' IMAGES AND WORK 6

ROLES AND RESPONSIBILITIES 6

PRINCIPAL 7
NETWORK MANAGER 7
DSL 8
STAFF 8
CHILDREN 9
PARENTS AND CARERS 9

ACCESS/COMPUTER LOGINS 9

PASSWORD POLICY 9

FILTERING AND MONITORING 10

CURRICULUM 11

HANDLING ONLINE SAFETY CONCERNS AND INCIDENTS 11

MAKING OR SHARING NUDES AND SEMI-NUDES, INCLUDING AI-GENERATED IMAGES 12
MISUSE OF SCHOOL TECHNOLOGY 12
SOCIAL MEDIA INCIDENTS 12

ARTIFICIAL INTELLIGENCE AND EMERGING TECHNOLOGIES 13

ACCEPTABLE USE OF AI 13
UNACCEPTABLE USE OF AI 13
ACADEMIC INTEGRITY AND TRANSPARENCY 14
DATA PROTECTION AND AI 14
AI LITERACY AND DIGITAL CITIZENSHIP 14
REVIEW OF EMERGING TECHNOLOGIES 15
APPROVAL AND ASSURANCE 15

PUBLICATION 15

LINK WITH OTHER POLICIES 16

KEY CONTACTS 16

Introduction

Online Safety (e-Safety) focuses on educating children and young people about the benefits and risks of using new technologies (including Internet technologies and electronic communications such as mobile phones and wireless devices), and on providing safeguards and awareness to help users control their online experiences. PORG International School's e-safety policy will operate in conjunction with other policies, including those for Safeguarding, Pupil Behaviour, Bullying, Data Protection and Security.

As a British School Overseas in the Czech Republic, the school uses Keeping Children Safe in Education 2026 (KCSIE 2026) as safeguarding good practice while complying with applicable Czech law and the EU General Data Protection Regulation. References to UK guidance in this policy inform the school's standards and procedures but do not displace local legal duties or reporting routes.

Purpose

The purpose of this policy is to establish a consistent whole-school approach to online safety, online platforms and artificial intelligence (AI). It aims to protect pupils, staff and families from online risks while supporting positive digital citizenship, digital wellbeing, safeguarding, privacy and responsible participation in the digital world.

The policy also provides clear expectations for the appropriate use of technology and helps ensure that all members of the school community understand their roles and responsibilities in maintaining a safe and supportive online environment.

Aim

We aim to ensure that children and young people are protected from harm and supported to derive the maximum benefit from new and emerging technologies, without risk to themselves or others.

Online Safety depends on effective practice at several levels:

- Responsible ICT use by all staff and pupils is encouraged by education and made explicit through published policies.
- Thoroughly implement online safety policy in administration and curriculum, including secure school network design and use.
- Safe and secure broadband, including effective content filtering.

An understanding of healthy and respectful relationships and appropriate boundaries; we consider effective PSHE to be a fundamental part of our approach to supporting pupils to grow into confident, caring, responsible and respectful young citizens.

The four areas of online risk

The school plans its safeguarding, curriculum, technical controls and incident response around the four interrelated areas of online risk identified in KCSIE 2026:

- **Content:** exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme violence, misinformation, disinformation and conspiracy theories.
- **Contact:** harmful interaction with other users or with generative-AI applications that simulate interaction, including peer pressure, grooming, exploitation, commercial targeting and adults posing as children.
- **Conduct:** behaviour that causes or increases the likelihood of harm, including cyberbullying and making, sending or receiving explicit images, including images altered or generated using AI.
- **Commerce:** online gambling, inappropriate advertising, phishing, scams, in-app purchases and other financial exploitation.

Digital technology

At PORG International School, Internet use is an integral part of everyday life for both pupils and teachers. It raises educational standards, promotes pupil achievement, supports staff professional work, and enhances the school's management and administration systems.

As part of the statutory curriculum, it is a necessity for effective learning. Access to the Internet is, therefore, an entitlement for pupils, who need guidance and development in a responsible and mature approach to its use. Our school has a duty of care to provide pupils with quality, safe Internet access.

The Internet is a powerful tool, and we actively encourage its usage outside of school. However, children will need to learn to evaluate and judge Internet information to protect their own safety and security.

Electronic communication

World Wide Web

If staff or pupils discover unsuitable sites, the URL (address), time, and content must be reported to the Principal, who will be able to add the site to the school filter list.
The school will ensure that the use of Internet-derived materials by pupils and staff complies with copyright law.
Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

Pupils may use only approved email accounts within the school system. Pupils must immediately tell a teacher if they receive an abusive email.

Pupils must not reveal personal details about themselves or others in email communication or arrange to meet anyone without specific permission.
If a whole-class or group email address is used in school, the teacher will monitor it.

Access to external personal email accounts at school may be blocked.
Emails sent to external organisations are carefully written and authorised by the class teacher before being sent, in the same way as a letter written on school-headed paper.
The forwarding of chain letters is not permitted.

Social Networking

We will block/filter access to social networking sites and newsgroups unless a specific use is approved.
Pupils are advised never to give out personal details of any kind which may identify them or their location.

Pupils are advised not to place personal photos on any social network space.
Pupils are advised on security and encouraged to set effective passwords, deny access to unknown individuals and instructed on how to block unwanted communications.

Video Conferencing

Video conferencing may be used to support teaching, learning, collaboration, assemblies, meetings, and communication with external organisations. All video conferencing activities must be conducted in a safe, secure, and age-appropriate manner.
To ensure online safety:

- Video conferencing sessions will be appropriately supervised according to the age and needs of the pupils.
- Only school-approved platforms and applications may be used for educational purposes.
- Meeting links, passwords, and access details must be shared securely and not distributed publicly.
- Staff must ensure that appropriate safeguarding and privacy settings are enabled, including waiting rooms, participant controls, and restricted screen sharing where necessary.
- Pupils are expected to behave respectfully and follow the school's behaviour and acceptable use expectations during online sessions.
- Recording of sessions by pupils is not permitted unless authorised by the school.
- Staff should use professional language, appropriate backgrounds, and maintain professional conduct at all times.
- Any safeguarding concerns, inappropriate behaviour, or security issues occurring during video conferencing sessions must be reported immediately to the Designated Safeguarding Lead (DSL).
- Parents and carers should support pupils in participating safely and appropriately in remote or online learning activities.

Managing Emerging Technologies

New technologies, platforms and AI tools must be assessed before school approval. The assessment will consider educational purpose, age suitability, safeguarding and wellbeing risks, privacy and data processing, security, accessibility, bias, intellectual property, supplier controls, filtering and monitoring limitations, and whether safer alternatives are available. Approval may be restricted, conditional or withdrawn.

The school is a mobile-phone-free environment for pupils by default throughout the school day, including lessons, transitions, break times and lunchtime. Any exception must be authorised by the Principal for a documented medical, accessibility, safeguarding or educational reason. Smart watches and other connected personal devices are subject to the same principle where they enable messaging, recording or internet access. Staff use must be professional, proportionate and consistent with the Staff Code of Conduct; personal devices must never be used to photograph or record pupils.

Published Content and the School Website

The contact details on the Website will be the school address, email and telephone number.

Staff or pupils' personal information will not be published.
The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully in accordance with Child Protection regulations.
- Publishing pupils' work, photographs, videos, and full names on the school's website, Blog, or Social Media, particularly when associated with images, is covered by the school's GDPR.
- For further information on taking and publishing images of children, please refer to our GDPR School Policy for the safe use of photographs.

Roles and responsibilities

Although overall responsibility for e-safeguarding rests with the principal, all e-safeguarding procedures outlined in this document assume the designation of named staff to the roles detailed below. It is the responsibility of the governing body and principal to take corrective and disciplinary measures as necessary when a breach of the Code of Conduct occurs and to contact and cooperate with police and other law enforcement agencies where a violation constitutes a criminal act.

Principal

- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote learning procedures, rules and safeguards.
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the DSL and ensure that the responsibilities listed are followed and fully supported.
- Ensure that all staff follow policies and procedures.
- Undertake training in offline and online safeguarding by statutory guidance.
- The DSL participates in all online-safety issues that might arise and receives regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security, ensuring the school's provision.
- Follows best practice in information handling; works with the staff, DSL and governors to ensure a GDPR-compliant framework for storing data but helps to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Ensure the school implements and makes effective use of appropriate ICT systems and services, including school-safe filtering and monitoring, protected email systems and that all technology, including cloud systems, is implemented according to child-safety first principles.
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures.
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including the risk of children being radicalised.
  Designate a senior leader responsible for filtering and monitoring and ensure that roles for the Principal, DSL, ICT Manager/IT provider and Proprietor are documented and understood.
  Ensure filtering and monitoring effectiveness is reviewed and recorded at least once each academic year and whenever a significant safeguarding risk, system change, new device, major update or generative-AI tool is introduced.
  Ensure the annual online-safety review is supported by a risk assessment reflecting pupils' ages, EYFS and Primary provision, SEND, EAL, vulnerabilities, technology use and relevant incidents.

Network manager

The network manager is responsible for the performance, security and error detection of the network. They also implement access controls; this is the responsibility of our IT Consultants. The Network manager will provide all pupils with a username and password, which will keep an up-to-date record of users and their usernames.

The ICT Manager and IT provider will maintain the technical filtering, monitoring, access-control and cyber-security arrangements; test them on all school-managed

internet-connected devices and relevant locations; provide reports and alerts promptly to the DSL and responsible senior leader; keep a log of checks, findings and actions; and verify coverage before new devices or services are deployed.

Technical controls must account, so far as reasonably possible, for real-time, dynamic, personalised and AI-generated content. Their limitations must be documented and mitigated through supervision, curriculum, configuration and reporting procedures.

DSL

The Designated Safeguarding Lead takes lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. The DSL works with the Principal, responsible senior leader and technical staff, reviews relevant monitoring reports, responds to alerts and concerns, contributes to risk assessments and annual reviews, ensures actions are recorded, and provides safeguarding assurance to the Proprietor.

Staff

- All staff will be given the school e-Safety Policy, and its importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- An audit of e-safety training needs will be included in the general ICT training needs review process. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme to ensure they fully understand the school's e-safety policy and Acceptable Use Policies.
- The Principal/Network manager will provide advice/guidance/training as required to individuals as required.
- Discretion and professional conduct are essential at all times.

Staff must understand their responsibilities for filtering and monitoring, supervise pupils appropriately, report any unsuitable content or system weakness promptly, and never attempt to bypass controls except through an authorised and recorded educational process.

Staff must not use personal or unapproved AI accounts for pupil data, safeguarding records, assessment decisions or confidential school information. AI output must never replace professional safeguarding judgement, direct observation, statutory or local reporting procedures, or consultation with the DSL.

Any AI-generated communication, resource or assessment material used with pupils must be checked by the responsible member of staff for accuracy, bias, age appropriateness, privacy, copyright and safeguarding risk before use.

The Proprietor will approve any significant changes to the PSHE policy and hold the principal to account for its implementation.

Children

- Children will be informed that Internet use will be monitored.
- A planned e-safety programme should be provided as part of ICT/PHSE/other lessons and regularly revisited – this will cover both the use of ICT and new technologies in and out of school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems/internet will be posted in all rooms and on individual laptop trolleys.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Parents and carers

- Parents' and carers' attention will be drawn to the school e-Safety Policy on the school website.
- They should consult with the school if they have any concerns about their children's and others' use of technology.
- They should promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing others' images or details without permission and refraining from posting harmful, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Access/Computer logins

Password Policy

Employee passwords are kept private, and only the holder can change them, although some of them can be reset by admin users both within the school (for some applications) and by the school's IT Consultants or other software providers.
It is good practice for users to change their passwords regularly.
Passwords must:

- be more than 8 characters long
- contain upper- and lower-case letters
- contain a number
- contain a special character (*&^%$)

Computers must not be left unattended in 'logged on' mode. Employees should lock their screens when they leave their desks.

Staff iPads should all be password-protected and locked when not in use.

Access to the network is restricted according to job role.

All users will have clearly defined access rights to school ICT systems. The Network

Manager will record details of the access rights available to user groups.

The Network Manager will provide all pupils with a username and password and will keep an up-to-date record of users and their usernames.

Filtering and monitoring

Filtering is preventative, and monitoring is reactive; neither replaces staff supervision, education or professional judgement. Controls will block harmful and inappropriate content without unreasonably restricting teaching, learning or pupils' development of digital resilience.

The Principal, DSL, ICT Manager/IT provider and Proprietor will review provision at least annually. The review will consider the school's pupil risk profile; what is blocked and allowed; user groups; school-managed devices and locations; remote access; emerging risks; incidents and alerts; use of generative AI; and whether systems can address dynamic, personalised and AI-generated content.

Checks will be completed and recorded at a frequency proportionate to risk and following significant changes. Records will state the date, the person completing the check, the devices, locations, and user profiles tested, the content or functionality checked, the findings, and the resulting actions. The school will verify that controls remain active and cover pupil, staff and guest accounts appropriately.

Concerns identified through monitoring must be reviewed promptly by the DSL or deputy and handled under safeguarding procedures. Staff and pupils must know how to report unsuitable content, false positives, missed content, alerts and suspected attempts to bypass controls.

Curriculum

E-safety should be a focus across all areas of the curriculum, and staff should reinforce e-safety messages when using ICT.

In lessons where internet use is pre-planned, it is best practice to guide pupils to sites checked as suitable for their use and to have processes in place for dealing with any unsuitable material found in internet searches.

While pupils are allowed to search the internet freely, e.g., using search engines, staff should be vigilant in monitoring the content of the websites young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network manager and the principal, if agreed, temporarily remove those sites from the filtered list for the duration of the study. Any request to do so should be auditable, with clear reasons for the need.

Pupils should be taught in all lessons to be critically aware of the materials/content they access online and to validate the accuracy of the information.
Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Handling online safety concerns and incidents

It is vital that all staff recognise that online safety is part of safeguarding and a curriculum strand of Computing and PSHE. General concerns must be handled in the same way as any other safeguarding concern.

This school commits to taking all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside the school and outside the school, and that those from outside the school will continue to impact pupils when they come into school or during extended periods away from school. School procedures for online safety are detailed in the Child Protection & Safeguarding policy and the Behaviour & Anti-Bullying Policy. All members of the school are encouraged to report issues promptly so we can address them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL on the same day. Any concern/allegation about staff misuse is always referred directly to the principal.

We will inform parents/carers of online safety incidents involving their children, and the Police, where staff or pupils engage in, or are subject to, behaviour that we consider particularly disturbing, or that breaks the law.
For specific online safety concerns, refer to the Child Protection and Safeguarding policy.

Making or sharing nudes and semi-nudes, including AI-generated images

Any concern involving the making, alteration, possession, request or sharing of a nude or semi-nude image of a person under 18 must be reported immediately to the DSL or Deputy DSL. This includes photographs, video, livestreams, digitally altered images and content wholly generated by AI, sometimes called deepfakes or deep nudes. It also includes threats, blackmail or financially motivated sexual extortion (sextortion).

Staff must not view, copy, print, forward, store, save or ask a pupil to download or resend the imagery. They should secure the device or account only where safe and necessary, preserve non-image evidence such as usernames, URLs, dates and the pupil's account in accordance with the safeguarding policy, and avoid promising confidentiality.

The DSL will make an immediate safeguarding and risk assessment, consider the child's wishes and vulnerabilities, protect all children involved, record the rationale and actions, and decide whether parents, Czech child-protection services, police or other specialist support should be involved. Parents will normally be informed early unless doing so may place a child at greater risk or prejudice an investigation. Children will never be blamed for victimisation, manipulation or coercion.

Misuse of school technology

Clear and well-communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on the school site and outside of school). Where pupils contravene these rules, the school behaviour policy will be applied; where staff violate these rules, action will be taken as outlined in the staff code of conduct/handbook. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology or the right to bring devices onto school property.

Social Media Incidents

When using social media in our school community, we have clear rules and expectations of behaviour for children and adults.
Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, we will request that the post be deleted and will expect this to be actioned promptly.

Artificial Intelligence and Emerging Technologies

The school recognises the growing role of artificial intelligence (AI) and emerging technologies in education, communication, and everyday life. AI tools may support creativity, research, organisation, accessibility, language development, and personalised learning when used responsibly.

The school is committed to ensuring that AI technologies are used safely, ethically, transparently, and in ways that support learning and wellbeing.

Generative AI can produce convincing but inaccurate, biased, harmful or manipulated content and can simulate human interaction. Its use must therefore be purposeful, supervised, age-appropriate and subject to the same safeguarding, filtering, monitoring, privacy and incident-reporting expectations as other online activity.

Acceptable Use of AI

Pupils and staff may use only school-approved AI tools for a defined educational or administrative purpose and within the access, age, supervision and account conditions set by the school. Pupil-facing use requires active teacher oversight. No pupil is required to create a personal account or provide unnecessary personal data to access an AI activity.

Examples of acceptable use include:

- Brainstorming ideas and research support
- Language translation and literacy support
- Revision and study assistance
- Coding and computational thinking support
- Accessibility support for diverse learning needs
- Drafting or organising ideas with proper acknowledgement
- Creative projects and innovation activities

Unacceptable Use of AI

The following uses of AI are prohibited:

- Submitting AI-generated work as entirely original work
- Using AI to cheat on assessments or examinations
- Generating harmful, offensive, discriminatory, or inappropriate content
- Creating fake images, videos, or impersonations intended to deceive or harm
- Sharing confidential, personal, or sensitive school information with AI systems
- Using AI tools to bully, harass, manipulate, or exploit others
- Circumventing teacher instructions or academic integrity expectations

- Creating, altering, requesting, possessing or sharing sexualised, nude or semi-nude content involving a child or identifiable member of the school community, including deepfakes or deep nudes
- Using AI companions, chatbots or simulated personas in ways that expose pupils to grooming, sexual content, coercion, dependency, self-harm encouragement or other harmful interaction
- Using AI for automated safeguarding conclusions, disciplinary decisions, admissions decisions or other high-impact decisions without accountable human review
- Attempting to bypass safety settings, age restrictions, filters, monitoring or school approval controls

Academic Integrity and Transparency

Students must:

- Follow teacher guidance regarding AI use.
- Acknowledge when AI tools have supported their work.
- Demonstrate their own understanding and learning.
- Verify the accuracy and reliability of AI-generated information.

Teachers may:

- Define when AI use is permitted or restricted.
- Require students to explain their learning process.
- Use plagiarism detection and authenticity checks where appropriate.

Data Protection and AI

Users must not enter:

- Personal student information
- Confidential school data
- Staff records
- Safeguarding records
- Health information,
- Special-category data
- Identifiable pupil work
- Photographs, recordings
- Credentials or other sensitive information into public or unapproved AI systems.

Any authorised processing must use the minimum necessary data, an approved account and supplier, a documented lawful basis and risk assessment, appropriate contractual and security controls, and human oversight.

AI Literacy and Digital Citizenship

The school will educate students about:

- How AI systems work
- AI bias and misinformation

- Ethical and responsible AI use
- Privacy and digital footprints
- Deepfakes and manipulated content
- Critical thinking and fact-checking

Review of Emerging Technologies

The school will regularly review emerging technologies and AI platforms to assess:

- Educational value
- Safeguarding risks
- Data privacy compliance
- Accessibility and inclusivity
- Impact on teaching, learning, and wellbeing

Only approved technologies may be used within the school environment.

Approval and assurance

Before approving an AI product, the school will consider the Department for Education's generative AI product safety expectations as good practice, including age assurance, safety-by-design, moderation and reporting features, privacy, security, transparency, human oversight, accessibility, and supplier responsiveness. Approval records will identify the owner, purpose, users, permitted data, safeguards, review date, and withdrawal process.

Approved tools remain subject to review. The school may suspend access immediately where an incident, safeguarding concern, material supplier change, data breach, ineffective control or new risk makes continued use unsafe.

Publication

The Online Safety Policy is available to all members of the school community, including teaching and non-teaching staff, parents, pupils, volunteers and relevant school personnel through the school information system and internal communication platforms. Hard copies are available upon request from the Principal's office.

The school is committed to ensuring that the policy remains accessible, transparent, and clearly understood across both EYFS and Primary provision, supporting effective communication, accountability, and positive partnership with families.

Link with other policies

Antibullying Policy
Behaviour Policy
Complaints Policy
Curriculum Policy
Mental Health and Wellbeing Policy
PSHE Policy
Remote learning policy
Safeguarding Policy

Key Contacts

ICT Manager	Jaroslav Filip	filip@porg.cz
Data protection manager	Michaela Comova	hotline@cca.cz
DSL and PSHE Coordinator	Thabang Lehner	lehner@porg.cz
Pastoral Care Lead	David Rojas	rivera@porg.cz
Principal	Barbora Gazdova	gazdova@porg.cz
Proprietor	Dagmar Dluhosova	dluhosova@porg.cz