Polish British Academy of Warsaw

Primary School

Online Safety Policy

Headmistress: Maria Fiedorczuk-Piechota (Y 0-3), Beata Belchowska (Y 4-8)

Governors: Magdalena Eysmont (DGS), Monika Konieczna-Kowalczyk

Designated Safeguarding Lead (DSL): Aleksandra Kuszaj

Approval date: 12th January 2024

Policy is: PUBLIC

Review date: January 2025

This policy should be read alongside Standards for the Protection of Minors.

Rationale

Polish British Academy of Warsaw recognises that children should be able to use the Internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

The policy applies to all staff, students, volunteers and anyone involved in the school activities.

Aims

- ensure the safety and wellbeing of students is of utmost importance when they are using the Internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

Strategy for implementation

The School will:

- provide clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- support and encourage the students to use the Internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- support and encourage parents and carers to do what they can to keep their children safe online
- develop clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a student
- review and update the security of our information systems regularly

- ensure that user names, logins, email accounts and passwords are used effectively
- ensure personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate (see Data Protection Policy)
- ensure that images of students are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- provide supervision, support and training for staff and volunteers about online safety
- examine and risk assess any social media platforms and new technologies before they are used within the organisation.

Dealing with online abuse

The school will:

- have clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- provide support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- make sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- review the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

At PBA, the following rules apply regarding the use of electronic devices, including those with internet access:

1. During school hours, students are not allowed to use mobile phones. Upon entering the school buildings, PBA students must deposit their phones at the reception desk and can retrieve them while leaving the school when classes have finished.

2. It is prohibited to record sound, images, or take photographs using mobile phones or other electronic devices on school premises.

3. The use of multimedia devices during educational activities is allowed if required by the course or curriculum, with the permission of the teacher.

4. In case of unauthorised use of mobile phones or other electronic devices by students, consequences outlined in the School Statute may be applied.

5. The school, while providing students with internet access, installs and updates software to protect students from accessing content that may pose a threat to their proper development.

6. Children's access to the internet on school premises is supervised by a teacher during IT lessons, extracurricular activities, and during after-school care.

7. Rules for internet use are outlined in the regulations available in the IT lab.

8. Teachers conducting lessons or supervising students are responsible for ensuring safe internet use by students.

9. All computers with internet access are equipped with and regularly updated:

- content-filtering software;
- software to monitor children's internet use;
- antivirus software;
- anti-spam software;
- a firewall.

10. A designated school employee checks if any harmful content is present on internet-enabled computers.

11. If harmful content is found, the employee identifies who used the computer at the time the content was introduced.

12. The school employee reports information about the child who used the computer when the harmful content was introduced to the Headmistress.

13. The Headmistress, along with a school counsellor or psychologist, discusses internet safety with the child.

14. If the counsellor or psychologist learns during the conversation that the child is being harmed, they take action in accordance with the school's established procedures.

15. The school conducts sessions for students on internet safety.

Procedures for protecting children from harmful content and threats on the internet or in other forms:

1. The main forms of cyberbullying include: harassment, threats, blackmail using the internet, publishing or distributing embarrassing or compromising information, photos, or videos via the internet, and impersonating someone online against their will.

2. In each case, when determining the circumstances, the nature of the incident must be established (extent and seriousness of the harm, whether it is a one-off or recurring event).

3. When implementing the procedure, actions that could further stigmatise the victim or the perpetrator should be avoided, such as calling a student out of class or confronting the victim with the perpetrator.

4. It should be assessed whether the incident constitutes cyberbullying or, for example, a poorly thought-out joke (in which case measures should be taken to prevent the escalation of such behaviour).

5. Evidence related to the act of cyberbullying should be secured (printouts, screenshots, web page records).

6. If the perpetrator of cyberbullying is known and is a school student, the school counsellor should have a conversation with them about their behaviour. This conversation should help establish the circumstances, understand the reasons behind the behaviour, and attempt to resolve the conflict.

7. The victim should be supported first. They must feel safe and cared for by adults. The child's sense of security is enhanced by knowing that the school is taking steps to resolve the issue.

8. When speaking with a student who reports being a victim of cyberbullying, reassure them that they are not to blame for the situation, that no one has the right to treat them this way, and that they did the right thing by disclosing the situation. Show understanding of their feelings, including the difficulties in revealing the details of the incident, fear, and shame.

9. Inform the child that the school does not tolerate violence and that appropriate intervention procedures will be implemented. The student should be informed about the steps the school can take and the ways to ensure their safety.

10. Support for the victim does not end when the procedure is completed. The situation should be monitored, ensuring the child's continued safety, such as observing whether any further bullying actions are being taken and how the child is coping within the group after the cyberbullying incident has been disclosed.

11. The parents/guardians of the victim should be kept informed of the situation, ensuring the child is treated as a subject. If the child does not consent, their concerns should be discussed, and if this does not help, refer to the rules and inform the parents. During discussions with the child and/or their parents/guardians, specialist support may be suggested (e.g., a school psychologist or a psychological-pedagogical counselling centre), as well as the possibility of reporting the case to the police.

12. The safety of witnesses to the incident should be ensured, especially if they disclosed the cyberbullying. During conversations with witnesses, empathy and understanding of their feelings should be shown, including fears of being labelled a "snitch" or fear of becoming the next victim.

13. The occurrence of cyberbullying does not necessarily require the involvement of the Police or the Family Court – the teacher's interventions should aim to resolve the problem at the educational level.

14. The school will notify the appropriate authorities (e.g., the Police, Family Court) when all available educational measures have been exhausted (talks with parents, applying the consequences outlined in the School Statute, psychological-pedagogical intervention).

15. The Police will be notified in cases where the law has been violated (criminal threats – Article 190 of the Penal Code, persistent harassment, impersonation –

Article 190a of the Penal Code, coercion to perform a specific action – Article 191 of the Penal Code, violation of sexual privacy, recording the image of a naked person without consent – Article 191a of the Penal Code, defamation – Article 212 of the Penal Code, insult – Article 216 of the Penal Code).

Procedure in case of suspicion that a child is participating in a dangerous game:

1. Check if the child has any signs of self-harm or other signs that may indicate participation in dangerous games. If necessary, provide medical or psychological care.

2. Under no circumstances delete any disclosed data in the form of messages (SMS, email, chat, etc.), as deleting such data may significantly hinder or even make further police procedures impossible. Obtain information about the child's online profiles, accounts, chats, etc., where relevant data for the case may be located.

3. Secure the content as much as possible by saving, printing, etc.

4. In a conversation with the child, determine the circumstances in which they learned about the game and joined it, and identify other participants with whom they were in contact during the game.

5. Report your suspicion to the school psychologist or counsellor, the Headmistress, and the child’s parents.

6. Report your suspicion to the Police, providing all available data, information, and circumstances of obtaining them. During police procedures, it may be necessary to provide the equipment on which such data is stored to secure essential information for further actions (such data will serve as evidence in preparatory proceedings).

Reporting cases of online abuse

The school recognises that it is not responsible for an official investigation. If the matter warrants reporting to the local authority, this will be in accordance with the Polish law.

Related documents:

Child Protection and Safeguarding Policy

Data Protection Policy