Policy:

Online Safety and Acceptable Use of Technology

1. Introduction

At Thames British School, we recognise the importance of fostering a safe and responsible online environment for all members of our school community. This policy aims to ensure the safety, security, and well-being of students, staff, and parents in the digital world. It reflects our commitment to equipping students with the knowledge and skills needed to use technology safely, responsibly and ethically.

This document outlines the expectations for responsible and appropriate use of technology, including devices, networks, software, and online platforms, within our school community. By following this policy, students ensure a safe, respectful, and productive learning environment for everyone. This policy applies to all students, staff, parents, guardians, and visitors who access the school's digital systems, networks, devices, or online platforms, both on and off the school premises. It also covers personal devices used for educational purposes.

This policy aligns with our commitment to excellence and transparency, as expressed in our guiding principles:

At Thames British School Warsaw, we **c | a | r | e**

Our Principles:
We care:

- that every one of our students reaches their full potential, academically, socially and emotionally;
- that every student is safe and feels safe at school, and this means we are all responsible all of the time;
- that communication and our choice of language is inclusive and respectful;

- about our behaviour and what it may communicate to others. We conduct ourselves in an ethical manner and with integrity at all times;
- about our communities culture, behave in a manner that fosters our values and insist that all members of our community do the same; and
- about learning first and foremost. Teachers are considered facilitators of learning and models for our community and its culture.

Our values:

c	**Collaborative & Compassionate**	We work together when needed to get the job done. We value the work of others, are compassionate, and recognise that success is mutually beneficial
a	**Authentic**	We are real, genuine and honest. We are true to ourselves and our community and represent our-selves as such with integrity
r	**Responsible & Resilient**	We have an obligation to reach our potential and fight to do so. We are accountable for our actions and utterances, and demonstrate respect for others needs and our environment. We don't give up.
e	**Enlightened**	We act on evidence, are factually well-informed, tolerant of alternative opinions, and guided by rational thought.

2. Objectives

- To promote a culture of responsible and safe use of the internet, devices, and digital tools.
- To protect students and staff from inappropriate or harmful content, cyberbullying, or online exploitation.
- To ensure compliance with legal and regulatory requirements regarding digital safety.
- To provide clear guidelines for acceptable online behaviour and the use of digital tools within the school community.

3. General Expectations

- Technology is to be used for administrative, educational purposes to support the learning process.
- Students are expected to use devices, the internet, and all digital tools responsibly, safely, and ethically.
- All users must respect the rights, privacy, and property of others while using technology.
- All members of the school community are expected to carry out their responsibilities with regards to online safety.
- Students should follow instructions from teachers and staff regarding technology use.
- All personal devices are the responsibility of the owner. The school does not take responsibility for damage or loss of the devices.
- All staff members and students are expected to follow procedures and communications provided by the IT department.

4. Responsibilities

4.1 School Leadership

- Ensure the implementation of the Online Safety Policy and provide adequate resources for training and monitoring.
- Ensure regular reviews of online safety measures are conducted.
- Support staff and students in dealing with any online safety incidents.
- Ensure all users are provided and agree to the acceptable use of this policy.

4.2 Teachers and Staff

- Promote safe and responsible online behaviour during teaching and learning activities.
- Supervise students' use of digital devices and online platforms during school hours.
- Report any incidents of cyberbullying, inappropriate content, or breaches of this policy to school leadership or DSL if safeguarding concerns are involved.
- Model appropriate use of digital tools and maintain professional online conduct.

4.3 Students

- Use the internet and school devices responsibly and for educational purposes only.
- Follow the school's Mobile Device Policy and Acceptable Use Policy for Technology.
- Report any concerns, cyberbullying, or inappropriate content to the Designated Safeguarding Lead, a teacher, or school counselor (psychologist).

- Protect their personal information and respect others' privacy and digital rights.

4.4 Parents and Guardians

- Support the school in promoting online safety at home by monitoring their child's internet usage.
- Encourage open conversations about online safety and responsible behaviour.
- Report any concerns or incidents to the school.
- Are responsible for private devices and software used for school activity.
- Are responsible for digital security incidents caused by their children provided they were done with malicious intent or by not following the school policy.
- Are accountable for material and intellectual property damage done by not following policies, instructions and communication laid out by the school staff.

4.5 IT Department

- Provide clear instructions and regulations on the usage of digital tools used by staff, students and their parents..
- Provide access to tools, accounts and services required for work and school activities.
- Conduct security audits periodically.
- Ensure a safe digital environment is provided in the school.

5. Common Online Threats

There are multiple online threats that may arise from non-compliance with the provisions of this policy. The list below is not exhaustive; these are just a few examples of the many ways cyberspace can be compromised. The landscape is constantly evolving, with new threats and tactics emerging regularly.

1. **Breaches**

    a. **Data breaches:** Unauthorised access to sensitive, protected, or confidential data resulting in theft of personal information, financial data or intellectual property.
    b. **Ransomware attack:** Malicious software encrypts the victim's data as the attacker demands a ransom to restore access. Can lead to significant financial losses, operational disruption and reputation damage.
    c. **Phishing attacks:** Deceptive attempts to obtain sensitive information by masquerading as a trustworthy entity via email or other communication channels. Often targets login credentials, financial information, or personal identification numbers.

d. **Malware:** Software designed to disrupt, damage, or gain unauthorised access to computer systems. Includes viruses, worms, Trojan horses, and spyware.
e. **Denial-of-Service (DoS) Attacks:** An attempt to make a machine or network resource unavailable to its intended users by overwhelming it with traffic.

2. **Violations**

a. **Privacy violations**: Unauthorised collection, use or distribution of personal information. Examples include unauthorised monitoring, data mining and breaches of data protection regulations.
b. **Intellectual property theft**: Unauthorised use or reproduction of someone else's intellectual property. Includes copying software, pirating media and stealing copyrighted information.
c. **Social Engineering**: Manipulating individuals into divulging confidential information or performing actions that compromise security.
d. **Identity theft**: Fraudulent use of someone else's personal information, often for financial gain. Can result in financial loss and damage to the victim's reputation.
e. **Cyberbullying**: Using online accounts to bully their victim. Very often done anonymously. Can cause damage to reputation and wellbeing.
f. **Credential Stuffing**: Using stolen usernames and passwords to gain unauthorised access to multiple accounts. Relies on the fact that many users reuse passwords across different sites.
g. **Insider threats**: Employees or students with legitimate access who misuse their access to harm the organisation or other people like teachers or students. Can lead to data breaches, intellectual property theft and many other security incidents.

6. Procedure for Dealing with Safety Incidents

1. **Don't Panic**: Stay calm and avoid making any rash decisions that could worsen the situation.

2. **Report the Incident**: Immediately report the incident to our IT department. Provide them with details about what you've observed (e.g., unusual activity, strange emails, or unusual system behaviour). You can contact the IT department via email at **it-support@thamesbritishschool.pl**, through the support portal at **it-support.thamesbritishschool.pl**, or directly.

3. **Disconnect from the Network**: If you notice suspicious behaviour, disconnect your device from the internet and any network (e.g., Wi-Fi or Ethernet).

4. **Avoid Clicking**: Do not click on any links or open files related to the incident (e.g., from phishing emails or suspicious pop-ups).

5. **Shut Down if Necessary**: If you suspect a serious breach (e.g., malware or ransomware), shut down your device to limit potential damage.

6. **Follow IT Department Instructions**: The IT team will guide you through the next steps. They may ask you to provide detailed information about the incident or give you specific instructions. Remember, the IT department will never ask for your credentials or login information.

7. **Don't Try to Fix It Yourself**: While it may be tempting to address the issue yourself, it's crucial to let the experts handle it. Attempting to resolve it on your own may unintentionally make the problem worse.

8. **Prioritise the Incident**: Reporting and handling safety incidents should take priority over other daily tasks for all parties involved.

7. Acceptable Use Guidelines

All users of the school's digital resources are expected to:

- Use school-provided devices, platforms, and school network for academic purposes only.
- Avoid sharing confidential credentials or accessing unauthorised systems.
- Refrain from accessing, creating, or sharing harmful, inappropriate, or illegal content.
- Respect intellectual property rights and avoid plagiarism.
- Never engage in cyberbullying, online harassment, or sharing offensive materials.

8. Personal and School Devices

- All pupils are obliged to comply with Mobile Devices Use Policy and this policy.
- Staff and pupils must ensure their devices are secure and used appropriately in line with GDPR regulations.
- **Primary School:** Pupils may use only school devices (e.g. desktop computers, Chromebooks) under teacher supervision. Personal devices are not permitted unless explicitly authorised.
- **High School:** Pupils may use personal devices (e.g. laptops, tablets) for educational purposes with permission and as per teacher instructions.
- All private devices need to be authorised and whitelisted for use by the IT department.
- The school reserves the right to monitor or restrict the use of personal devices if misuse occurs.

9. Internet Use

- Access to the internet must be for educational and work or school-related activities only.
- Students and staff must not visit inappropriate websites, including those containing violence, explicit content, illegal activities, gambling, and arms trade. The school reserves the right to decide on what sites and services are deemed appropriate at any given time.
- Respectful communication must be maintained in all online spaces (e.g., emails, chats, forums).
- Pupils are responsible for reporting any accidental access to inappropriate material to a teacher who will report the concern to the DSL. The DSL will record the incident and take action as per The Safeguarding and Child Protection Policy.
- DSL is responsible for reporting all accidental access incidents reported to them to the IT department.

10. Responsible Use of School Platforms and Software

- Pupils are allowed to use school-provided accounts, platforms, and software only for educational purposes.
- School systems must not be used for downloading unauthorised software or other content.
- Pupils should save their work regularly and keep files organised.
- All software and digital services should be provided by the IT department.
- Usage of privately owned accounts and services needs to be pre authorised by the IT department.
- All new services and applications should be provided and configured by the IT department.

11. Acceptable use of school-owned online accounts

- All school owned accounts must meet the minimum password complexity rules established by the IT department.
- All user accounts should be protected with multi factor authentication always when applicable.
- Access to Google accounts (used also to access other systems) of students will be granted by their guardians/parents themselves by resetting it via predefined personal email address and the forgotten password form until the student reaches the age of 18 years old.
- All accounts have confidential status. Sharing access to an account to a third party without authorization is forbidden.

- Usage of online accounts is allowed only for educational and work-related purposes.

12. Use of Technology in Classrooms

- Technology use must be appropriate and aligned with the teacher's instructions.
- Devices should not distract students from learning. During lessons, unnecessary use (e.g., games, social media) is not permitted.
- Devices such as computers or Chromebooks must be turned off or put away when not in use or when instructed by a teacher.

13. Care for Devices

- Pupils must handle school devices with care to avoid damage.
- Use of school owned devices by students should be supervised by teachers.
- Borrowing school devices should be supervised by the teachers and reported to the IT department.
- Relocating school owned devices should be done after approval from the IT department.
- Food and drinks cannot be kept near devices.
- Any damage or malfunction students report to a teacher who then promptly notifies IT staff through appropriate channels (it-support@thamesbritishschool.pl).
- If High School pupils are permitted to use their personal laptops or iPads, they are expected to ensure their devices are fully operational and charged for use during class.

14. Consequences for Misuse

Misuse of technology will result in appropriate consequences, which may include:

- Verbal warnings or reminders.
- Temporary retrieval of student's device (returned to parents or guardians).
- Parental notification and involvement.
- Further disciplinary action in line with the school's behaviour policy.
- Disciplinary action towards employees which may result in financial fees, termination of contract and legal action.

15. Online Safety and Security

15.1 Expectations of pupils

- Pupils must never share personal information (e.g., full name, address, phone number, passwords) online outside of authorised school systems.
- Passwords must be kept confidential and not shared with others.
- Pupils should not attempt to bypass or disable school security settings, filters, or monitoring tools.
- Report any suspicious or harmful online activity, cyberbullying, or security issues to the DSL immediately.

15.2 Online Safety Education

- The school will provide education for students and staff regarding:
  - Cybersecurity risks and safe internet usage practices.
  - Identifying and reporting cyberbullying, online abuse, and inappropriate content.
  - Privacy protection and managing personal information.
  - Responsible use of social media, email, and other digital tools.
  - Promoting digital citizenship and ethical behaviour in an online world.
- All teachers are expected to participate in internal professional development offered at school.
- All teachers are expected to complete the Online Safety Act course on EduCare.

15.3 Filtering, Monitoring, and Security

- The school will maintain secure firewalls and filtering systems to block access to harmful or inappropriate content.
- Digital activity on school devices and networks will be monitored to ensure compliance with this policy.
- Any breaches or attempts to bypass security measures will be addressed immediately.
- All school owned devices will be managed by the IT department.
- All software installed on the school devices will be managed by the IT department including ransomware protection, vulnerability patching and security updates.
- School networks will be divided depending on their usage case into:
  - Staff network - only for school owned devices used by the staff.
  - Student network - used only by authorised student and school owned devices.
  - IT Lab network - used only by specialised IT lab room devices.

    - Visitor network - used by authorised third party personnel, guests and personal devices.
- All mobile school devices will have its data encrypted.

16. Cyberbullying and Online Abuse

- Cyberbullying and any form of online abuse will not be tolerated under any circumstances.
- Pupils found engaging in such behaviour will face disciplinary measures as per the Student Accountability and Responsibility Guidelines and Anti-Bullying Policy.
- Victims of cyberbullying will be supported through counselling and safeguarding protocols.

17. Reporting Online Safety and Security Incidents

All members of the school community are required to report any online safety concerns or incidents immediately to:

- The Designated Safeguarding Lead (DSL)
- School leadership
- IT support (it-support@thamesbritishschool.pl)

The school will investigate all reports and take appropriate action in line with safeguarding and disciplinary procedures.

18. Safeguarding and Data Protection

The school is committed to ensuring all data, including students' personal information, is protected in line with **GDPR** and other applicable regulations. Staff and students must:

- Protect confidential and sensitive information.
- Avoid sharing personal data online without consent.
- Use only school provided and authorised data storing services and devices.

19. Consequences of Policy Violations

Failure to comply with this policy may result in:

- Revoked or suspended access to school networks and devices.

- Disciplinary actions as per Student Accountability and Responsibility Guidelines.
- In severe cases, involvement of external authorities.

20. Policy Review

This Online Safety Policy will be reviewed periodically or as needed to reflect technological changes, emerging risks, and updates in legal requirements.

21. Related Policies

- Safeguarding and Child Protection Policy
- Mobile Devices Policy
- Student Accountability and Responsibility Guidelines
- Anti-Bullying Policy
- Staff, Volunteers and Contractors Code of Conduct