AZBUKA Russian-English bilingual school
E-safety policy and practice

PERSON RESPONSIBLE:	Head Teacher/DSL
Approved by:	Governors of AZBUKA Foundation
Approved:	September 2024
DATE OF NEXT REVIEW:	**July 2025**

We recognise the exciting opportunities technology offers to staff and children in our setting and have invested in age appropriate resources to support this belief. While recognising the benefits we are also mindful that practitioners have a duty of care to ensure that children are protected from potential harmful online material and that appropriate filtering and monitoring systems are in place.

To reflect our belief that when used appropriately and safely, technology can support learning, we encourage adults and children to use a range of technological resources for a wide range of purposes. At the same time, we do all we can to ensure that technology is used appropriately and that children are safeguarded against all risks. While it is not possible to completely eliminate risk, any e-safety concerns that do arise will be dealt with quickly to ensure that children and staff adhere to safe practices and continue to be protected. We will communicate our safe practice in the use of technologies with families, and manage any concerns.

1. Scope of the policy

This policy applies to everyone- staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. The policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site. **We aim to**:

- Raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many learning and social benefits
- Maintain a safe and secure online environment for all children in our care.
- Provide safeguarding protocols and rules for acceptable use to guide all users in their use of technology and online experiences
- Ensure all adults are clear about sanctions for misuse of any technologies both within and beyond the early years setting.

2. Hardware and provision use

Internet provision, all computers and AZBUKA IT devices are maintained and monitored by a professional IT contractor (company – "ACTIVE IT"). The School governors together with the IT contractor will put in place strengthened measures to protect children from harm online - including cyber bullying, pornography and the risk of radicalisation.

This includes:

- Cloud Filtering (applies to all web activity and devices using our network whether owned by the school or not). Controlled by OpenDNS (Cisco)
- Router Filtering (applies to all web activity and devices using our network whether owned by the school or not), Controlled By Sonicwall (Dell)
- Workstation filtering (installed on all PC's and laptops that belong to the school, does not include I- Pads), Controlled by Sophos (Anti Virus)
- Enforcing google **safe search** on the entire network.

Additionally, to meet the **Filtering and Monitoring Standards for Schools and Colleges**, our filtering provider is:

*a member of Internet Watch Foundation (IWF)
*signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
*blocking access to illegal content including child sexual abuse material (CSAM)

Our filtering system is operational, up to date and applied to all:

*users, including guest accounts
*school owned devices
*devices using the school broadband connection

Our filtering system:

*filter all internet feeds, including any backup connections
*be age and ability appropriate for the users, and be suitable for educational settings
*handle multilingual web content, images, common misspellings and abbreviations
*identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
*provide alerts when any web content has been blocked

Our filtering systems allow us to identify:

*device name or ID, IP address, and where possible, the individual
*the time and date of attempted access
*the search term or content being blocked

We also meet the requirements for **Cyber Security in Schools**, see https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

Where staff have been issued with a device (e.g. setting laptop, desktop or iPad) for work purposes, personal use whilst off site is not permitted unless authorised by the provider/manager. Staff taking photographs or recording with technology not owned by our setting is specifically not allowed.

All staff have a shared responsibility to ensure that children are supervised when using the internet and related technologies to ensure appropriate and safe use as part of the wider duty of care and responding or reporting promptly issues of concern.

Setting issued devices only should be used for work purposes and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted.

When personal devices are temporary used for work purposes, only encrypted memory sticks must be used for all work related files. All data must be transferred to setting computers/servers as soon as possible.

Online searching and installing/downloading of new programs and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device.

Setting issued devices should not leave the premises unless encrypted and this must be acknowledged in the policy. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting.

3. Data storage and management

No electronic documents that include children's and families personal confidential information (including child protection records) will be transported out of the setting e.g. on Fobs, memory sticks.

Setting issued devices should not leave the premises unless encrypted. In the case of an outing, all data must be transferred/deleted from the setting's camera/device/temporary device before leaving the setting and/on arrival back in school.

4. Email

The setting has access to a professional email account to use for all work related business, including communication with parents/carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

Staff must not engage in any personal communications (i.e. via hotmail or yahoo accounts etc.) with parents of children who they have a professional responsibility for.

Staff should not participate in any material that is illegal, obscene and defamatory or that is intended to annoy or intimidate another person or persons.

All emails should stay professional in tone and checked carefully before sending, just as an official letter would be. Care should be taken when forwarding emails from others.

5. Social Networking

Employees must not access personal blogs/social networking sites on work premises or use the setting's internet systems or email address for their own use, without prior agreement or in accordance with the setting's policy.

The designated teachers and staff can post photos, video and write posts related to teaching and learning content ONLY on the official AZBUKA FB page, website and Instagram/other Azbuka and School accounts and according to school policies and practice. The setting does not condone employees writing about their work on social networking sites or web pages. If employees choose to do so, they are expected to follow the rules below.

Staff must not:

- disclose any information that is confidential to the setting or any third party or disclose personal data or information about any individual child, colleague or service user, which could be in breach of the Data Protection Act.
- Post photos of children and premises.
- link their own blogs/personal web pages to the setting's website.
- make defamatory remarks about the setting, colleagues or service users.
- misrepresent the setting by posting false or inaccurate statements.

Communication with children and young people, by whatever method, should always take place within clear and explicit professional boundaries. Staff should avoid any misinterpretation of their motives or any behaviour that could be construed as grooming.

Staff should not: send social networking site ‘friend requests’ to, or accept them from, children or parents who use the setting.

Failure to adhere to the rules and guidelines in this policy may be considered misconduct and could lead to disciplinary and /or criminal investigations.

Remember that anything posted online could end up in the public domain to be read by children, parents or even future employers – so be careful what you post and who you post it to. For example, posting explicit pictures of yourself could damage your reputation and that of your profession and organisation. Parents and employers may also question your suitability to care for children.

6. Sanctions

Misuse of technology or the internet may result in:

- the logging of an incident
- disciplinary action
- reporting of any illegal or incongruous activities to the appropriate authorities
- allegations process being followed

7. Linked policy: AZBUKA Safeguarding Policy (2023-2024)