

## Acceptable Use Policy for Technology

### *Our Charter of Good Digital Technology Behaviour at Aspen Heights British School.*

All daily usage of the computer network, including the Internet and Email activity, is subject to monitoring by the school.

When I use digital technologies, I agree to be a safe, responsible, and ethical user at all times, by:

- Accessing only my own account and not attempting to access others' accounts.
- Interacting respectfully with others online and in the Aspen Heights British School community, refraining from engaging in online bullying or disrespectful behavior.
- Seeking appropriate permissions and acknowledging the use of others' work when creating content.
- Not capturing or sharing pictures, videos, recordings, or any content of anyone in the Aspen Heights British School community without explicit teacher instruction.
- Respecting copyright and intellectual property laws when conducting research and presenting my work.
- Reporting any inappropriate use of digital technology, including their own devices, by other students to a teacher.
- Safeguarding my privacy and promptly informing a teacher if I encounter requests for personal information or feel uncomfortable or unsafe online.
- Respecting the privacy of others by refraining from sharing their personal information without their consent.
- Immediately notifying a teacher if I suspect unauthorised access to my account.
- Informing a teacher if I receive online contact from someone I do not know.
- Avoiding interference with network systems and security, tampering with another user's data, or attempting to access the network using another student's credentials.
- Adhering to guidelines on downloading and using programs, seeking teacher permission when necessary.
- Refraining from publishing or uploading any information about Aspen Heights British School or anyone in the Aspen Heights British School community.
- Avoiding access to inappropriate material or engaging in unauthorised activities such as gaming or social media during school hours.
- Using email solely for educational purposes as instructed by teachers.
- Handling Aspen Heights British School's IT devices with care and promptly notifying a teacher if any damage or issues arise.

## Policy:

### Purpose:

To ensure all students at Aspen Heights British School use technology ethically, responsibly, and safely to enhance learning while protecting themselves and others.

### Scope:

This policy applies to all Aspen Heights students, covering the responsible usage of school-owned and personal devices.

### Basic Safety:

- Students may only use iPads, Chromebooks, or internet browsers during lessons—and only for educational purposes.
- A child must ask for permission before using any device during classes and social times. Social networking sites, personal email accounts, and video calling services are strictly off-limits during the school day.
- In line with UAE Federal Decree-Law No. 5/2012, Art. 21 (now superseded by No. 34/2021, Art. 44), it is illegal to invade others' privacy using digital technology—this includes taking photos, videos, or audio recordings without consent.
- All recordings made during school hours must be approved by a teacher beforehand. Our server actively blocks access to restricted or inappropriate websites.
- Any attempt to bypass these restrictions will be logged, and the incident reported directly to the IT department and school leadership.
- Students are strictly prohibited from using or carrying mobile phones anywhere on campus, under any circumstances.
- Smartwatches with their own internet connectivity are not permitted.
- Students are forbidden from accessing material that is profane, obscene, or promotes illegal behaviour, violence, or discrimination.
- If inappropriate material is accessed—even accidentally—students must report it immediately to a teacher or staff member.
- The use of Virtual Private Networks (VPNs) is strictly banned to prevent circumvention of content filters and maintain safe, controlled internet access.
- Students must not make deliberate attempts to disrupt the computer system or destroy data.
- Students may not alter school hardware in any way.

### Emails:

- Every student is provided with an Aspen Heights email account. This must be used exclusively for communication within Aspen Heights.
- Personal email accounts (e.g., Gmail, Hotmail, Yahoo!) must **never** be used to contact Aspen Heights staff.
- Students should not use their school email for personal matters—e.g., signing up for outside platforms or chatting with friends.
- Y1 and Y2 generic emails

- Access to personal email or any messaging platform is not allowed during the school day.
- All emails sent from school accounts must be polite, respectful, and considerate of differing views—no inappropriate or aggressive language.
- If you receive an email sent in error, notify the sender immediately and inform a teacher if needed.
- Any email containing violent, dangerous, racist, discriminatory, defamatory, or inappropriate content must be reported to a staff member immediately.

**Policy Breach:**

- Any breach of this policy will result in appropriate disciplinary action as per the ADEK breaches.
- Consequences following the Relationship Policy may be invoked by the teacher within the classroom. The use of devices at school is a privilege that can be revoked.
- Inappropriate use of devices can result in limits to or loss of use of the devices at school.

**To ensure technology and digital learning is safe, appropriate and purposeful, the following will be completed:**

**Annual Digital Audit & Governance**

- Conduct a full digital audit at the beginning of each academic year to assess current practices and infrastructure.
- Form a Digital Governance Team, comprising senior leadership, IT staff, teachers, and student/parent representatives, to drive digital strategy.
- Develop and review annually a whole-school digital strategy emphasising purposeful, safe, and balanced technology use.

**Staff Professional Development**

- Provide ongoing, role-specific professional development for staff—covering digital pedagogy, cybersecurity basics, cloud and MDM tools.
- Identify and empower departmental digital champions to support and mentor peers.

**Technical Infrastructure & Security**

- Deploy and maintain Mobile Device Management (MDM) with student-level settings and updates.
- Enforce firewall restrictions and access controls tailored for student devices and content filtering.
- Regularly audit technical systems (devices, Wi-Fi, licenses, access logs) to ensure secure and efficient operation.

**Student Digital Habits & Wellbeing**

- Host student workshops and assemblies focused on reflecting on digital habits, setting healthy screen-time goals, and raising awareness of online safety.

- Schedule regular "Unplugged" days, encouraging screen-free learning and balanced device use.
- Incorporate digital citizenship and cyber-safety education into the curriculum—covering privacy, cyberbullying, and critical thinking.

#### **Parent & Community Engagement**

- Offer Tech Clinic sessions or drop-in opportunities for parents to build their confidence with school platforms and devices.
- Collect feedback through parent surveys or forums to understand their needs and experiences with school technology use.