BLOOM WORLD ACADEMY

Reference Number
BWA-12

Acceptable Use Policy	
Audience and coverage	*School community*
Published where	*Staff handbook* and school website
First release date	November 2022
Last reviewed	September 2025
Next review	August 2026
Owner	Nicola Upham, Principal – Well-being and Development
Reviewer	John Bell, Executive Principal 

BLOOM WORLD ACADEMY

1. Aim

Bloom World Academy (BWA) considers this policy to be:

- an essential part of the school;
- supportive to staff and students in managing certain situations;
- an important framework that will ensure consistency in applying values and principles throughout the establishment;
- a roadmap for day-to-day operations;
- compliant with laws and regulations, gives guidance for decision-making, and streamlining internal processes;
- designed to influence and determine all major decisions, actions and all activities taking place within the boundaries set by them;
- aligned to the school's guiding statements and identified goals which are formed in strategic leadership meetings.

2. Statement of intent

BWA believes this policy to be a working document that is fit for purpose, represents the school ethos, mission and vision, enables consistency and quality across the school and is related to the relevant UAE legislation.

3. Scope

This policy applies to all stakeholders in the Academy.

4. Unique definitions

A shared understanding of the following definitions are integral to the implementation of this policy, and as such staff should endeavour to use the correct terminology at all times.

5. Processing and practice

The follow narrative is explicit in its guidance, consistency, accountability, efficiency, and clarity on how the school operates with regard to E-safety procedures

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff and visitors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

BLOOM WORLD ACADEMY

The Four Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, sharing other explicit images and online bullying
- **Commerce** – risks such as inappropriate advertising, phishing and/or financial scams

Legislation

BWA is guided by the best practice established by the UK DfE specifically the statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff
- Searching, screening and confiscation
- protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

How is online safety taught?

Students will be taught about online safety using guidance from the UK National curriculum.

In **KG2 - Grade 1**, students will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Find a balance between online and offline activities
- Staying safe while accessing a website or an app

Students in **Grades 2 - 5,** will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Identify the importance of leaving behind a responsible digital trail
- Identify the rights and responsibilities we have as creators
- Identify how to keep online friendships safe

By the **end of Junior School**, students will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Grades 6 - 8,** students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- Finding credible information on the internet
- Understand how to respond to cyberbullying

Students in **Grades 9 - 12** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- How to respect the privacy of others online
- Online reputations and friendships
- Challenging our own conformation bias

By the **end of Senior school**, students will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, and how and when consent can be withdrawn (in all contexts, including online)
- Media addiction
- Health effects of screen time
- Digital footprint that showcases your purpose

The safe use of social media and the internet will also be covered in other subjects where relevant.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SoD.

Electronic Addiction

To promote healthy digital habits, prevent electronic addiction, and support students who may be struggling with compulsive device use, in alignment with the school's safeguarding responsibilities.

Prevention & Education

Whole-School Approach:

- Embed digital wellness into computing, and health education curricula.
- Use age-appropriate psychoeducation to teach students about:
    - The addictive design of apps and games.
    - Impacts on brain development, sleep, mental health, and relationships.
    - Strategies for self-regulation and healthy screen habits.

Digital Wellness Programs:

- Implement school-based prevention programs that include:
    - Emotion regulation and critical thinking skills.
    - Motivational enhancement strategies (e.g., goal-setting, digital contracts).
    - Peer-led discussions and reflection activities.

Device Use Boundaries:

- Clear expectations are shared with all students for device use during instructional hours.

- Tech-free zones created; no devices at lunchtimes, no phones contracts in place for Senior students unless at end of the school day for pick up.

Support for Students with Signs of Addiction

Identification & Referral:

- All Staff trained to recognise signs of digital overuse (e.g., withdrawal, irritability, loss of interest in offline activities).
- Students raised in TAC (Team around Child meetings) to refer students where necessary

Intervention Strategies:

- Conduct a digital use assessment with the student and family.
- Develop a personalised support plan, which may include:
    - Scheduled device breaks.
    - Screen time monitoring tools.
    - Counselling sessions focused on emotional regulation and coping strategies.

Family Engagement:

- Share resources and guidance with parents on managing screen time at home.
- Host parent workshops on digital wellness and parenting in the digital age.

Defamation on Social Media

To educate students and staff about the legal and ethical implications of defamation on social media, and to ensure compliance with UAE laws that criminalise defamatory online behaviour.

Legal Framework

Defamation in the UAE is a **criminal offense**, governed by:

- **Federal Decree-Law No. 31 of 2021 (Penal Code)** – Articles 425–428
- **Federal Decree-Law No. 34 of 2021 (Cybercrime Law)** – Article 43
- **UAE Student Conduct Bylaw** – prohibits defamatory content targeting individuals or institutions

Key Legal Points:

- Defamation includes **false statements** that harm a person's **reputation, dignity, or honour**, whether written, spoken, or shared digitally.
- **Social media posts**, even on private accounts, are considered **public dissemination** under UAE law.
- **Intent is not required** — even well-meaning or sarcastic posts can be prosecuted if they cause reputational harm.
- Penalties include **fines up to AED 500,000**, **imprisonment**, and **deportation for expats**.

BLOOM WORLD ACADEMY

School Expectations & Education

Student Education:

- Digital citizenship lessons will include:
  - What constitutes defamation.
  - UAE legal consequences of online misconduct.
  - Respectful communication and conflict resolution online.

Staff Training:

- Safeguarding and pastoral teams will be trained to:
  - Identify online defamation risks.
  - Support students involved in incidents.
  - Liaise with legal and parental stakeholders appropriately.

Acceptable Use Agreement:

- Students must agree not to:
  - Post or share defamatory content about peers, staff, or the school.
  - Circulate rumours, memes, or screenshots that ridicule or harm others.
  - Repost private messages or images without consent.

Response to Defamation Incidents

Safeguarding Protocol:

- All incidents will be treated as **serious safeguarding concerns**.
- The Designated Safeguarding Lead (DSL) will:
  - Investigate the incident.
  - Inform parents and relevant authorities if necessary.
  - Provide support to both victims and perpetrators.

Restorative Approach:

- Where appropriate, the school will use restorative practices to:
  - Help students understand the impact of their actions.
  - Promote accountability and reconciliation.

BLOOM WORLD ACADEMY

Legal Referral:

- In severe cases, the school may refer incidents to:
  - **Dubai Police Cybercrime Unit**
  - **Legal counsel** for further action

Guidelines for AI Use

- AI outputs must be fact-checked and not used to target or misrepresent individuals or institutions.
- AI-generated or altered videos/images of students, teachers, or any community member must not be created, shared, or published without their explicit permission and knowledge.
- AI tools must not be used to manipulate, edit, or fabricate images/videos in a way that could cause reputational harm, bullying, or defamation within or outside the school community.

Response to Defamation Incidents (AI-related)

- Report incident immediately to Safeguarding Lead
- Assess nature and impact of the AI-generated content.
- Request takedown/remove harmful content.
- Investigate source and intent of misuse.
- Provide support to affected student/staff.
- Apply disciplinary measures as per school policy.
- Record incident in log for compliance and follow-up.
- Escalate to KHDA/UAE authorities if severe.

Cybersecurity Policy

Guidelines

- All student and staff data must be stored securely on approved school platforms only.
- Sensitive files must not be transferred through personal emails or personal devices.
- Students and staff are strictly prohibited from attempting to hack or bypass school security systems.
- Altering, deleting, or corrupting school records, files, or assessments is a serious violation.
- Users must avoid connecting to unsecured public Wi-Fi when accessing school resources.

User Access Levels:

- Access to school systems and data is granted based on the principle of least privilege; users receive only the permissions necessary to perform their roles.
- Different user groups (e.g., students, teachers, administrators, IT staff) have defined access levels with specific rights and restrictions.

- Administrative access is limited to authorised personnel only and requires additional authentication measures.
- Access rights are regularly reviewed and updated, especially when users change roles or leave the school.
- Users must not attempt to access areas or data beyond their authorised level.

Response to Security Breach

- Any suspected cybersecurity breach must be reported immediately to the IT/Safeguarding team.
- IT team will investigate the incident, log details, and take corrective action.
- Disciplinary measures will be applied for violations, and serious breaches may be escalated to KHDA or UAE authorities.
- All incidents are monitored, recorded, and reviewed to prevent future breaches.
- Conduct post-incident reviews and update policies or staff/student training to reduce future risks.

Cyber-bullyiing

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power (further details provided in the behaviour for learning and Anti-bullying policy.

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This will be through forum assemblies as well as discussions in their homeroom time. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

BLOOM WORLD ACADEMY

Examining Electronic Devices

The SLT and Deputy DSL's can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other students and staff
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, a suitable response is discussed between the staff member, DSL and the Executive Principal. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child, they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next, seeing support from the police and external agenices.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Acceptable Use of the Internet in School

All Students, parents, staff, volunteers and BWA Advisory board members are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see appendices). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, BWA Advisory board members and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements (see appendices).

Students using Mobile Devices in School

Mobile phones and items such as smart watches, headphones, air pods etc, should not be used in school.

Students may bring mobile devices into school if they need to make contact with parents to arrange transport collection after school.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

How the School Will Respond to Issues of Misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour for learning and mobile phone policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff and MOE staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation

.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of images, especially around chat groups

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse

- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputies DSL will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

Monitoring Arrangements

In addition to the filtering provided by UAE telecoms provider, BWA will install the Smoothwall Monitoring Tool on all school owned devices. This service identifies and flags instances of inappropriate use, or that deemed to be a safeguarding concern.

Triggers:

- Inappropriate images, video or other content deemed illegal by the TRA
- Content linked to radicalisation/extremism
- Bypassing blocked content
- Pornography, nudity and vice
- Impersonation, fraud and phishing
- Insult, slander and defamation
- Invasion of privacy
- Offences against the UAE and public order
- Supporting criminal acts and skills
- Drugs
- Medical and pharmaceutical practices in violation of the laws
- Infringement of intellectual property rights
- Discrimination, racism and contempt of religion
- Viruses and malicious programs
- Promotion of or trading in prohibited commodities and services
- Illegal communication services
- Gambling
- Terrorism

- Prohibited top level domains
- Illegal activities
- Upon order from judicial authorities or in accordance with the law

Upon a keyword being triggered on a school-owned device the content will be ranked for level of concern and a screenshot taken of the web browser. If the content is flagged as very high risk, a member of the school safeguarding team will be contacted.

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

The data is analysed fortnightly with the Deputy DSL, to identify any re-occuring themes to determine additional training needs for staff and learning opportunities for students.

6. Roles and responsibilities

With regard to implementation of this policy roles and responsibilities are clearly stated below:

Role of the BWA Governing Board

It is the responsibility of the BWA Advisory board to:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

Role of the Executive Principal

It is the responsibility of the Executive Principal to:

- Ensure that staff understand this policy, and that it is being implemented consistently throughout the school.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Role of the Designated Safeguarding Lead (DSL)

It is the responsibility of the Designated Safeguarding Lead (DSL) to:

- Support the Executive Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the Executive Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged within CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3) contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Executive Principal/BWA Advisory board

Role of ICT Manager

It is the responsibility of the ICT manager to:

- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conduct a full security check and monitoring the school's ICT systems on a fortnightly basis
- Block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files
- Ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Role of Digital Leads (Junior and Senior)

- Ensure consistent implementation of the Acceptable Use Policy across Junior and Senior phases, supporting staff and students in following agreed expectations.
- Monitor digital practices within the school, identifying risks such as cyberbullying, inappropriate content, or misuse of AI, and escalating concerns to the DSL/ICT Manager.
- Lead on digital wellbeing initiatives, promoting balanced and responsible use of technology among staff and students.
- Provide training, guidance, and updates to colleagues on online safety, digital citizenship, and ethical AI use.

- Collaborate with the ICT Manager and Safeguarding Team to review filtering, monitoring, and reporting systems, ensuring they remain effective and up to date.
- Act as the key point of contact for digital safety matters within their phase, liaising with staff, students, and parents as required.

Pastoral Grade Leaders

- Ensure students in their grade understand and follow the Acceptable Use Policy through assemblies, tutor sessions, and ongoing reinforcement.
- Monitor digital behaviour within their grade, responding to incidents of online misuse, cyberbullying, or harmful conduct in line with the behaviour and safeguarding policies.
- Act as the first point of contact for staff and parents regarding digital safety or misuse concerns within their grade.
- Support the DSL by logging incidents on CPOMS and escalating safeguarding risks promptly.
- Promote positive digital citizenship, wellbeing, and balanced use of devices through grade-wide initiatives.
- Provide feedback to SLT and Digital Leads on emerging trends, risks, or training needs specific to their grade.

School Counsellors

- Provide direct support to students affected by online harm, cyberbullying, screen addiction, or misuse of digital platforms.
- Work with the DSL and Digital Leads to assess risk and put in place appropriate interventions or referrals.
- Deliver preventative education sessions on digital wellbeing, resilience, and safe online practices.
- Support staff and parents in understanding the emotional and psychological impacts of online risks, offering strategies for intervention.
- Maintain accurate, confidential records of digital safety cases in line with safeguarding protocols.
- Contribute to whole-school digital wellness initiatives, ensuring student voice and wellbeing remain central.

Role of Staff

It is the responsibility of all staff, including contractors, and volunteers to:

- Maintain an understanding of this policy
- Implement this policy consistently
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (and ensuring that students follow the school's terms on acceptable use

- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Role of the Parents

It is the responsibility of the parents to:

- Notify a member of staff or the Executive of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Role of the Students

It is the responsibility of the students to:

- Meet the terms included on the acceptable use of the school's ICT systems and internet (appendices 1 and 2)

7. Associated documentation

When implementing a policy consideration must be given to how it aligns and supports other policies. To ensure consistency this policy is fully aligned with the following key policies:

- Safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

This policy will be reviewed every year by the Principal – Well-being and Development. At every review, the policy will be shared with the BWA Advisory board. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

8. Training implications

This policy will be shared with all BWA academic and administrative staff in the staff handbook. Staff will be trained and /or refreshed at the start of each academic year – during the annual BWA induction week. For new joiners they will be walked through the policy by the Principal during their induction period.

9. Policy Review

This policy will be revisited by the ICT manager and Principal – Well-being and Development annually in readiness for the new academic year or amended as necessary in real time.

10. Safeguarding

We are committed to safeguarding and promoting the welfare of all children as the safety and protection of children is of paramount importance to everyone in this school. We work hard to create a culture of vigilance and at all times we will ensure what is best in the interests of all children.

We believe that all children have the right to be safe in our society. We recognise that we have a duty to ensure arrangements are in place for safeguarding and promoting the welfare of children by creating a positive school atmosphere through our teaching and learning, pastoral support and care for both students and school personnel, training for school personnel and with working with parents. We teach all our children about safeguarding.

We work hard to ensure that everyone keeps careful watch throughout the school and in everything we do for possible dangers or difficulties. We want all children to feel safe at all times. We want to hear their views of how we can improve all aspects of safeguarding and from the evidence gained we put into place all necessary improvements.

9. Equity Impact Assessment

We have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief.

This policy has been equality impact assessed and we believe that it is fair, it does not prioritise or disadvantage any member of staff or student and it helps to promote equality at this school.

BLOOM WORLD ACADEMY

Senior School AI Acceptable Use Policy (Grades 6–12)

Artificial Intelligence (AI) is a powerful tool that can support student learning. At Bloom World Academy, we encourage students to use AI responsibly, ethically, and transparently to enhance, not replace, their own thinking and creativity.

Principles of AI Use

- *AI can help you learn* – Using AI to research, brainstorm, check grammar, or explore different viewpoints is acceptable.
- *AI cannot do the work for you* – Submitting AI's work as your own is unacceptable.
- *Be transparent* – Always acknowledge when and how you used AI.
- *Your understanding matters* – You must be able to explain and show your own learning, not just repeat what AI produced.

Acceptable Uses of AI:

Students may use AI to:

- Summarise key points for research or essays (but explain them in their own words).
- Explore counterarguments, perspectives, and ideas for deeper understanding.
- Suggest essay structures or templates as a starting point.
- Seek feedback or suggestions in non-assessed contexts (classwork, practice tasks).
- Support creativity or inspiration.

Unacceptable Uses of AI:

Students must not use AI to:

- Generate whole essays, reflections, or projects and submit them as their own.
- Create research questions or coursework topics without teacher input.
- Copy AI-suggested quotes or references without verifying and reading them.
- Translate work into another language for assessed submissions.
- Rewrite or "rephrase" entire assignments through AI for submission.
- Hide or lie about using AI.

Referencing and Transparency

- If you use AI to generate text, ideas, images, or code, you must acknowledge this in your work.
- For major assessments, prompts and outputs may be required as an appendix.

Teacher Guidance:

- Teachers may ask students to explain or orally defend their work.
- If a teacher suspects over-reliance on AI, the student may be asked to redo the task under supervision.
- Drafts and process work should be saved to show evidence of authentic learning.

Consequences of Misuse:

- Using AI dishonestly is treated as a breach of academic integrity.
- Depending on severity, consequences may include resubmission, loss of credit, or disciplinary action.

BLOOM WORLD ACADEMY

Appendix 1: KG2 and Grade 1 acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Name of student:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• I will use AI safely and responsibly
• I will not delete school apps and will not change important settings
• I will not take pictures of or record others without their permission
• I will only use my device during lessons and will put my device away when instructed
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
• I will be kind and not share mean or hurtful things about friends, teachers, or our school.
• I will not share stories, pictures, or jokes that make others feel sad or embarrassed.
• I will only share pictures or messages if everyone in them says it's okay.
 	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and will make sure my child understands these. I understand and am aware of the software installed by the school to protect and safeguard the welfare of the students.	
Signed (parent/carer):	**Date:**

BLOOM WORLD ACADEMY

Appendix 2: Grades 2-12 acceptable use agreement (students and parents/carers)

Our Agreement
1. **We will model responsible and safe use of our own devices and accessories.** - I will take good care of my device, its screen, case, and accessories to avoid damage. - I will not remove or damage any cases or accessories provided by the school. - I may change wallpapers or device backgrounds only if it is appropriate and does not disrupt learning or distract others. - We will bring in headphones suitable for listening to educational material and only use them if a teacher asks us to. - Our mobile phones must never be seen out during school hours, anywhere on campus. If we need to speak to our parents, I must ask a teacher to use the school telephone. - The device provided to us is our own responsibility and I will take steps to keep it safe when we are at school. - It is our responsibility to make sure our devices are clearly labelled, and that there are no passcodes used on the devices. - The use of our devices in the corridors and at break time is disrespectful to the people around me because I am not being a fully attentive and present community member. We will not use them in these places. - We will not lend our device to anyone, even our friends. This is to keep our individual digital footprint safe. -
2. **We will ensure the use of our device is for the benefit of our learning.** - We will listen to our teacher's instructions and use our devices in class to further our subject knowledge and skills. - We will use our devices in designated learning areas only, to further our quest for knowledge. - We will connect to online learning classrooms when requested, as an agreement from myself to my teacher that I am dedicating my device to learning when I am in their classroom. - We will refrain from playing non educational games at school because this distracts myself and people around me and negatively impacts my ability to socially interact with the friends around me. - We will refrain from the use of unblocked games websites to access non educational games.
3. **Monitoring and Software Security** - I understand that the school installs monitoring and security software on my device to keep me safe. - I will not remove, disable, or tamper with any monitoring or security software installed by the school. - I understand that the school may check my device remotely to ensure compliance with this agreement.
4. **We will show our community that we are responsible citizens.** - We will not use a VPN for schoolwork because this is illegal in the UAE.

BLOOM WORLD ACADEMY

- We will not take photos or videos of people at school or in digital learning environments (no screenshots or recordings of video conferences), unless a teacher gives us permission and I also have the permission of the people in the photo or video.
- We will not intentionally steal or copy anyone's work online. This includes directly copying/pasting or using AI without properly referencing the original source.
- I will use the internet and browsers responsibly, avoiding websites or content that are inappropriate or harmful.
- I will not view, share, or download inappropriate images, videos, or language on my device.
- I will not post or share defamatory, harmful, or disrespectful content about peers, staff, or the school.
- I will not circulate rumors, memes, or screenshots that ridicule, embarrass, or harm others.
- I will not repost or share private messages, images, or videos without the explicit consent of all individuals involved.

5. **We will use AI safely and responsibly.**

- I will use AI tools responsibly to help with my learning.
- I will always be honest about when I use AI and will not use it to cheat or avoid doing my own work.

6. **Use of School Wi-Fi and Mobile Hotspots**

- I will only connect to the school's Wi-Fi network for learning purposes.
- I will not use unauthorised mobile hotspots or other internet connections on my device during school hours.
- Using mobile hotspots to bypass school internet controls is not allowed.

7. **We will be mindful of our own digital wellbeing and the wellbeing of others.**
   - I understand that at any time, a teacher may ask to look at the contents of my device or my Microsoft Account to ensure the safety and wellbeing of myself and others.
   - I understand that taking and uploading photos or videos of others on to social media without their consent is a finable offence in the UAE.
   - I understand that my actions in my digital environment can lead to reactions in my physical environment. I will treat everyone with respect.
   - I will ensure I do not support damaging material by "liking" or "reposting" it.
   - We will be mindful of our own digital footprint and only post on social media accounts if:

- I am over the required age of consent
- It is a post that is to the benefit, not to the detriment of others

8. **We are responsible learners and digital citizens no matter where we are in the world- Online Learning**
   - I will ensure I keep the privacy of myself and those around me. I will join online lessons with my video and microphone turned off and turn it on when instructed by the teacher.
   - I will always be in the presence of a teacher when conversing online- just like when I am in school in a real classroom! We will not be in a video meeting without a teacher.

BLOOM WORLD ACADEMY

- I will not send emails to the whole school or large groups without permission from a teacher or staff member. - I will use comment sections, chat, and other online communication tools respectfully and appropriately. - I will not post or comment anything hurtful, disruptive, or inappropriate in online school spaces. - We will be mindful of the importance of downtime and ensure that our learning and online messaging takes place no later than 6pm.
We understand that breaking Our Agreement will mean that there will be consequences for me according to our school behaviour agreement: What I have done will be recorded and a relevant sanction according to the seriousness of my behaviour will be put in place by a school staff member, teacher, senior leadership team or any academy staff as appropriate.

BLOOM WORLD ACADEMY

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is, offensive, obscene or otherwise inappropriate (and contrary to UAE laws and customs)
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Attempt to work around blocks or measures put in place to protect the student network and devices.

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (student):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

I understand and am aware of the software installed by the school to protect and safeguard the welfare of the students.

Signed (parent/carer):	**Date:**

BLOOM WORLD ACADEMY

Appendix 3: acceptable use agreement (staff, BWA Advisory board members, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
Name of staff member/BWA Advisory board/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of students using any personal devices • Share confidential information about the school, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too. <u>Teacher AI Use – Agreement</u> **When using AI tools in school, or outside school, I will not use them in ways that compromise student data, academic integrity, or my professional responsibility as a teacher.** As a teacher, I agree to use AI responsibly and ethically in line with school policy. • I will protect student data. I will never upload names, student records, photos, or any personal student information into AI tools.

• I will put humans first, AI second. I may use AI for planning and ideas, but not for grading, assessment, or final feedback. My professional judgement will always come first. • I will stay accountable. If I use AI for lesson planning or support, I will check the accuracy, bias, and suitability of all outputs before using them. • I will model ethical use. I will encourage students to question, verify, and think critically about AI outputs.	
Signed (staff member/BWA Advisory board/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, BWA Advisory board members and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	