



# Online Safety Policy

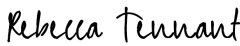
Policy Details

|                       |                      |
|-----------------------|----------------------|
| Policy Title          | Online Safety Policy |
| Policy Number         | EDUC-013             |
| Policy Owner          | Education Department |
| Version               | 2                    |
| Effective Date        | 1 August 2026        |
| Scheduled Review Date | 31 July 2028         |
| Applicable To         | All                  |

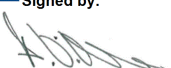
Prepared by:

| Name          | Designation                               | Signature                                                                                                                              |
|---------------|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Brendon Owens | Computing Teacher & Digital Learning Lead | <div>Signed by:<br/><br/>7B7B42408DFD4B0...</div> |

Reviewed by:

| Name              | Designation                     | Signature                                                                                                                                  |
|-------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Rebecca Tennant   | Head of Taaleem Teaching School | <div>Signed by:<br/><br/>FED92834770C45F...</div>     |
| Nicki Williams    | Director of Education           | <div>Signed by:<br/><br/>FE710AD974C54E2...</div>     |
| Graham Paris      | Director of Dubai Schools       | <div>Signed by:<br/><br/>63BB048DA7D24FB...</div>     |
| Nicola Neethling  | Charter Schools Director        | <div>Signed by:<br/><br/>D91E20FE178F4A5...</div>     |
| Natasha Pardasani | Head of Compliance              | <div>DocuSigned by:<br/><br/>0D63CBA9319B4B2...</div> |

Approved by:

| Name            | Designation             | Signature                                                                                                                            |
|-----------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Rebecca Gray    | Chief Education Officer | <div>Signed by:<br/><br/>AA0F895E3534450...</div> |
| Alan Williamson | Chief Executive Officer | <div>Signed by:<br/><br/>A88F8F28883242C...</div> |

## Table of Contents

| Section No. | Section Title                                          | Page No. |
|-------------|--------------------------------------------------------|----------|
| 1           | Purpose                                                | 4        |
| 2           | Related Policies                                       | 4        |
| 3           | Scope                                                  | 4        |
| 4           | Regulatory Context                                     | 5        |
| 5           | Key Terms                                              | 5        |
| 6           | Online Safety As Safeguarding                          | 6        |
| 7           | Roles And Responsibilities                             | 6        |
| 8           | Acceptable Use Agreements (AUA)                        | 8        |
| 9           | Staff Conduct And Use Of Social Media                  | 8        |
| 10          | Education And Prevention                               | 9        |
| 11          | Student Participation and Voice                        | 9        |
| 12          | Digital Wellbeing                                      | 10       |
| 13          | Technical Safeguards                                   | 11       |
| 14          | Emerging Technologies and Artificial Intelligence (AI) | 11       |
| 15          | Reporting and Responding to Concerns                   | 12       |
| 16          | Monitoring                                             | 13       |
| 17          | Implementation Timeline                                | 13       |
| 18          | Non-Compliance                                         | 13       |
|             | Appendix A: Unified Acceptable Use Agreement Template  | 14       |

# 1. Purpose

Taaleem Holdings PJSC (hereafter referred to as “Taaleem” or the “Company”) is committed to safeguarding and promoting the welfare of all children and young people. Online safety is recognised as a fundamental aspect of safeguarding and child protection and applies to all members of the school community.

Online safety encompasses the safe, responsible, ethical and appropriate use of digital technologies, including emerging technologies such as Artificial Intelligence (AI), and applies across all digital environments in which students and staff engage.

The purpose of this policy is to:

- protect students and staff from online harm, including risks associated with evolving technologies such as AI-generated content, impersonation, and data misuse
- provide clear expectations for the safe, ethical, and responsible use of technology
- promote digital citizenship, critical awareness, and wellbeing in an increasingly connected and AI-influenced world
- ensure compliance with UAE legal frameworks, safeguarding requirements, and regulatory expectations
- establish a consistent minimum standard for all Taaleem schools

## 2. Related Policies

Online safety should be considered within each school’s wider approach to digital learning, safeguarding, digital wellbeing, infrastructure, and emerging technologies which are included (but not limited to) in the policies below:

- Artificial Intelligence in Education Policy
- Information Security Policy
- Cybersecurity Policy
- Data Protection Policy
- Safeguarding & Child Protection Policy
- Behaviour Policy

## 3. Scope

This policy applies to all members of the school community, including students, staff, volunteers, visitors, and any other individuals using school systems, devices, or digital platforms.

It applies to all use of digital technology associated with the school, including emerging technologies such as Artificial Intelligence (AI).

This includes, but is not limited to:

- school-owned devices and platforms

- Bring Your Own Device (BYOD) arrangements
- personal devices accessing school systems or networks
- remote and home learning environments
- school-related online communication and digital interaction
- the use of AI tools and digital platforms that generate, manipulate, or share content

This policy applies both on-site and off-site where digital behaviour has the potential to impact safeguarding, wellbeing, or the reputation of the school community. All users are expected to always follow this policy alongside the school's Acceptable Use Agreements and relevant Taaleem policies.

## 4. Regulatory Context

This policy is aligned with relevant national legal frameworks and regulatory expectations relating to safeguarding, digital safety, data protection, and the responsible use of technology.

This includes:

- UAE Federal Decree-Law No. 34 of 2021 on Combatting Cybercrime
- UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data
- UAE Federal Decree-Law No. 26 of 2025 on Child Digital Safety
- KHDA / ADEK safeguarding and digital safety expectations

Schools must ensure that online safety practices remain aligned with applicable and evolving legal, safeguarding, and regulatory expectations.

## 5. Key Terms

For the purposes of this policy:

**Online Safety** refers to the safe, responsible, ethical, and appropriate use of digital technologies to protect users from harm and promote positive digital participation.

**Digital Wellbeing** refers to the balanced and healthy use of digital technologies in ways that support learning, relationships, personal development, and overall wellbeing.

**Artificial Intelligence (AI)** refers to digital systems or tools capable of generating content, analysing information, supporting decision-making, or responding to user input through machine learning or other computational processes.

**Safeguarding Concern** refers to any concern that a child or young person may be at risk of harm, abuse, neglect, exploitation, or unsafe digital interaction, including concerns arising through online activity or emerging technologies.

**Emerging Technologies** refers to new or developing digital tools, platforms, or systems that may create new opportunities or risks for students, staff, or the wider school community.

## 6. Online Safety as Safeguarding

**All online safety concerns, including those involving Artificial Intelligence (AI) and emerging technologies, must be appropriately assessed in the first instance to determine whether they constitute safeguarding or behavioural concerns, and managed in accordance with the relevant policies and procedures.**

All online safety concerns that constitute safeguarding concerns must:

- be reported to the Designated Safeguarding Lead (DSL) without delay
- be recorded on CPOMS or the school's approved safeguarding recording system

Online safety concerns may relate to:

- **Content** – exposure to harmful, inappropriate, or misleading material, including AI-generated content
- **Contact** – unwanted or unsafe communication, including impersonation or AI-assisted interaction
- **Conduct** – behaviour that causes harm or risk, including the creation or sharing of harmful or manipulated content (e.g. deepfakes)
- **Commerce** – financial exploitation, scams, or misuse of digital platforms

Where appropriate, concerns involving AI-generated content<sup>1</sup> (e.g. impersonation, manipulation, or misinformation) must be assessed and managed with the same level of seriousness as other safeguarding / behaviour risks.

Schools must ensure that patterns of concern are identified and reviewed as part of safeguarding oversight, including those that may emerge through repeated incidents or across groups of students.

Where online safety concerns indicate a wider technical or platform-related risk (e.g. filtering, monitoring, or system vulnerabilities), these must be escalated through appropriate channels, including liaison with Taaleem Central Office IT where required.

## 7. Roles and Responsibilities

Online safety is a shared responsibility across the whole school community, led by School SLT.

### Taaleem Education (Group Level)

The Central Education team at Taaleem is responsible for:

- setting minimum online safety expectations for all schools
- maintaining and reviewing this policy
- providing guidance and support to schools

<sup>1</sup> Further guidance on the safe and responsible use of AI is provided in the Taaleem Artificial Intelligence in Education Policy and school-level AI Implementation and Guidance.

- ensuring alignment with safeguarding, legal, and regulatory frameworks

### School Leadership Teams (SLT)

School leaders must ensure that:

- DSL has clear oversight of online safety
- online safety is fully embedded within safeguarding practice
- clear reporting processes are in place and understood by all staff
- staff receive regular online safety training in line with Taaleem's safeguarding expectations. This includes induction, annual updates, and additional training in response to emerging risks
- school systems and processes align with Taaleem expectations
- periodic online safety information, guidance or awareness opportunities are provided to parents and guardians where appropriate
- appropriate school level procedures, guidance and controls are maintained to support implementation of this policy

### Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- leading on all online safety concerns as safeguarding matters (if applicable)
- ensuring all concerns are recorded and managed in line with safeguarding procedures
- identifying patterns, trends, or emerging risks, including those linked to AI and digital technologies
- working with school leadership and, where appropriate, Taaleem Central Office to respond to online safety risks

## All Staff

All staff must:

- follow the school's Acceptable Use Agreement
- model safe, responsible, and professional online behaviour
- maintain appropriate professional boundaries in digital environments
- report any online safety concerns immediately to the DSL or school SLT
- remain vigilant to emerging risks, including those associated with AI-generated or manipulated content

## Students

Students must:

- follow the school's Acceptable Use Agreement
- use digital technologies responsibly and safely
- report concerns to a trusted adult
- understand that misuse of technology, including AI tools, may be treated as a safeguarding and/or behavioural concern

## Parents and Carers

Parents and carers are partners in online safety and are expected to:

- support safe and responsible use of technology at home
- reinforce school expectations where appropriate
- engage with school guidance and communication relating to online safety
- support safe and appropriate digital behaviour outside school, including responsible use of emerging technologies such as AI

## 8. Acceptable Use Agreements (AUA)

All members of the school community are required to follow the school's Acceptable Use Agreements (AUA), which define clear expectations for the safe, responsible, and appropriate use of technology.

This includes:

- student Acceptable Use Agreements
- staff Acceptable Use Agreements
- any relevant agreements for parents, visitors, or device use (e.g. BYOD)

Acceptable Use Agreements are implemented and managed at school level and must align with this policy and the Taaleem AI in Education Policy.

Schools are responsible for ensuring that:

- AUAs are age-appropriate and clearly understood
- expectations are communicated effectively to all users
- agreements are reviewed regularly to reflect emerging technologies, including AI
- appropriate processes are in place to obtain and maintain acknowledgement of applicable AUAs by relevant users

AUAs form part of the school's wider safeguarding and digital governance framework and should be read in conjunction with this Policy.

A sample AUA template is provided in Appendix A that can be amended by each school as required.

## 9. Staff Conduct and Use of Social Media

Online safety includes the professional conduct of staff in digital and online environments.

Staff must maintain appropriate professional boundaries in their use of technology and social media, including when using personal accounts. Online interactions, communications, and published content must not place students or staff at risk or undermine safeguarding principles.

Expectations relating to staff online conduct and social media use are set out in the **Taaleem Staff Code of Conduct and Taaleem Social Media Policy**, which must be read in conjunction with this policy.

Any concerns arising from staff online conduct, digital interactions, or social media activity that may impact safeguarding, student welfare, or the reputation of the school must be reported and managed through the appropriate safeguarding, HR, or disciplinary processes.

## 10. Education and Prevention

Online safety education is a core element of preventative safeguarding.

All Taaleem schools must ensure that online safety is explicitly taught and embedded across the curriculum in an age-appropriate and progressive manner.

This includes:

- teaching students how to use digital technologies safely, responsibly, and respectfully
- developing students' understanding of online risks, including those associated with emerging technologies such as Artificial Intelligence (AI)
- promoting critical thinking, including the ability to question, evaluate, and respond to online content
- providing guidance on privacy, social media use, digital reputation, and respectful online communication
- supporting students to recognise and respond to risks such as misinformation, manipulation, and harmful content

Online safety education must reflect the evolving nature of digital technologies and ensure that students are prepared to navigate increasingly complex online environments, including those influenced by AI-generated or manipulated content.

Schools retain autonomy over how this education is delivered, provided that provision is:

- age-appropriate
- progressive across phases
- regularly reviewed for effectiveness

Online safety education may be delivered through curriculum subjects, pastoral programmes, assemblies, or other school-led initiatives. Schools should maintain appropriate records or evidence of online safety education activities to support safeguarding oversight, continuous improvement, and regulatory or inspection requirements.

## 11. Student Participation and Voice

Taaleem recognises that students play an important role in helping schools understand the rapidly evolving digital landscape. Schools should actively seek and value student voice as part of their ongoing approach to online safety and digital wellbeing.

Students are often among the first to identify emerging technologies, online behaviours and digital trends. Their experiences and perspectives can help schools respond proactively to emerging risks, review existing practice and strengthen online safety provision.

Student participation may include:

- Digital Leaders or other student leadership opportunities
- Student councils, focus groups or consultation activities
- Student surveys and feedback
- Online safety campaigns and awareness initiatives
- Discussion and feedback on emerging technologies, including Artificial Intelligence (AI)

Schools should use student voice, where appropriate, to:

- evaluate the effectiveness of online safety education
- identify emerging risks and trends
- inform the continuous development of school practice
- promote a positive culture of responsible digital citizenship

Schools retain autonomy over how student participation is facilitated, provided that opportunities are meaningful, age-appropriate and contribute to the ongoing development of online safety provision.

## 12. Digital Wellbeing

Digital wellbeing forms part of Taaleem's broader commitment to safeguarding, student welfare, and personal development.

Taaleem recognises that digital technologies are embedded in learning, communication, and social interaction. While technology provides significant educational and social benefits, excessive, inappropriate, or unbalanced use may adversely impact mental health, sleep, relationships, academic engagement, and overall wellbeing.

All Taaleem schools must promote a balanced and responsible approach to the use of digital technology and support students in developing healthy digital habits.

Schools must:

- promote awareness of the impact of digital technologies on wellbeing, including social media use, online influence, and digital comparison
- support students in developing healthy routines and boundaries around screen time and online engagement
- encourage respectful and positive digital interactions and relationships
- help students understand how online content, including AI-generated or manipulated content, may influence perceptions, expectations, and behaviour
- respond appropriately where digital use impacts wellbeing or safeguarding

Digital wellbeing provision should be age-appropriate, progressive, and responsive to emerging trends in technology and student behaviour.

Schools retain autonomy over how digital wellbeing is delivered, including through curriculum provision, pastoral systems, assemblies, parent engagement, or student-led initiatives.

### 13. Technical Safeguards

Taaleem schools must ensure that appropriate technical safeguards are in place to support online safety and protect users from harm.

Schools are responsible for:

- ensuring that appropriate filtering, monitoring, and technical controls are implemented in accordance with Taaleem IT and cybersecurity requirements
- remaining vigilant to how systems operate in practice
- identifying any gaps, limitations, or emerging risks
- reporting concerns promptly through appropriate channels

Where issues are identified (e.g. inappropriate content access, over-restriction, attempts to bypass systems etc), these must be reported to the school IT team in the first instance. Where required, concerns will then be escalated to Taaleem Central Office IT for review and action.

All technical safeguards are subject to review by the Taaleem Central Office to ensure they remain effective, proportionate, and responsive to associated risks.

### 14. Emerging Technologies and Artificial Intelligence (AI)

Emerging technologies, including AI, present both opportunities and risks within the context of online safety.

Taaleem recognises that AI is increasingly shaping how students access information, create content, and interact online. This includes the potential for AI-generated or manipulated content, misinformation, and new forms of digital misuse.

Schools must ensure that students are supported to:

- understand the risks associated with emerging technologies
- critically evaluate digital content, including identifying inaccuracy, bias, or manipulation
- use technology in a safe, responsible, and ethical way

AI-generated or AI-edited images, audio, or video content involving students, staff, or members of the school community must comply with existing safeguarding, consent, digital media, and professional conduct expectations.

*This policy does not replace the Taaleem AI Policy or school-level AI Implementation and Guidance. These documents provide detailed expectations for the use of AI across teaching, learning, and professional practice.*

*Schools must ensure alignment between this Online Safety Policy, the Taaleem AI Policy, and their own AI Implementation and Guidance to maintain a consistent and safeguarding-led approach.*

As technologies continue to evolve, schools must remain responsive to emerging risks and adapt their practice accordingly.

## 15. Reporting and Responding to Concerns

All concerns relating to online safety must be taken seriously and responded to promptly.

Online safety concerns may give rise to safeguarding, behavioural, academic integrity, IT, cybersecurity, data protection, or other school-related matters. Following initial assessment, concerns shall be managed in accordance with the relevant school policies and procedures.

Online safety concerns may include:

- exposure to inappropriate or harmful content
- online bullying, harassment, or misuse of digital platforms
- misuse of AI tools
- attempts to bypass filtering or monitoring systems
- sharing or creation of harmful or manipulated content (e.g. deepfakes)

### Types of concerns and reporting

Where there is any uncertainty regarding the nature or severity of a concern, staff must treat the matter as a safeguarding concern and report it accordingly.

- **Safeguarding-related online safety concerns**, including those involving Artificial Intelligence (AI), must be reported immediately to the Designated Safeguarding Lead (DSL) and recorded using the school's safeguarding recording system (e.g. CPOMS or equivalent). Such concerns shall be managed in accordance with the Taaleem Safeguarding and Child Protection Policy and school safeguarding procedures.
- **Behaviour-related online safety concerns** that do not meet safeguarding thresholds should be recorded and managed in line with the school's Behaviour policy and procedures.
- **Where online safety concerns relate to technical systems** (e.g. filtering, monitoring, cybersecurity, or platform access), these must also be reported to the school IT team and escalated to Taaleem Central Office IT where required.
- **Other online safety concerns** like digital incidents that do not meet safeguarding thresholds should still be recorded through the school's appropriate behaviour, pastoral, IT, or incident reporting systems to support oversight, trend analysis, and auditability where appropriate.

Where there is any uncertainty regarding the level of concern, staff must treat the matter as a safeguarding concern and report it accordingly.

*Schools may provide additional guidance on escalation pathways and levels of response within their procedures to support consistency. This may be included within an appendix where appropriate.*

**Schools should maintain local procedures to support the investigation and management of online safety incidents. This should include, where appropriate, the preservation of evidence, communication with parents or carers, and engagement with external agencies in accordance with safeguarding, legal and regulatory requirements.**

## 16. Monitoring

Online safety is monitored through existing safeguarding, leadership, and school improvement processes across Taaleem schools.

The Senior Leadership Team (SLT), in conjunction with the Designated Safeguarding Lead (DSL), maintains oversight of online safety within the school. This includes:

- responding to concerns reported through safeguarding or behaviour systems
- identifying trends, patterns, or emerging risks in student and staff digital use
- ensuring alignment with Taaleem policies, including safeguarding and AI expectations
- supporting the ongoing development of staff awareness and practice

Where relevant, insights from technical systems (e.g. filtering and monitoring) may inform this oversight, in collaboration with school IT teams and Taaleem Central Office IT.

Monitoring is focused on identifying themes and improving practice, rather than routine surveillance of individual users. They will be proportionate, risk based and compliant with all relevant safeguarding, legal and data protection requirements.

## 17. Implementation Timeline

This policy shall be implemented within thirty (30) days from the Effective Date indicated on the cover page, allowing adequate time for communication, training, and adoption across all relevant Taaleem entities. Where any requirement in this policy is dependent on a system functionality, configuration, or tool that is not yet implemented, such requirement shall take effect only once the relevant functionality is operational. Until such time, existing processes shall continue to apply.

## 16. Non-Compliance

Non-compliance with any established corporate policies may result in disciplinary action.

## Appendix A – Unified Acceptable Use Agreement Template

**[School Name]**

### Whole School Acceptable Use Agreement (AUA)

At [School Name] we are committed to providing a safe, respectful, and purposeful digital learning environment.

This Acceptable Use Agreement applies to all users of school systems, devices, and networks, including students, staff, and guests.

- **Students should read Section 1 in full.**
- **Staff should read Section 2.**
- **Guests should read Section 3.**

***By accessing our systems or networks, you agree to follow the expectations outlined in the section that applies to you.***

### Section 1 – Students

#### Digital Responsibility

- I will use technology at school only when instructed and for learning purposes.
- I will be respectful in all digital communication and will not use rude, aggressive, or offensive language.
- I will never engage in cyberbullying, online harassment, or anything that may harm or upset others.
- I will not create, manipulate, generate, or share AI-produced images, videos, audio, or content (including “deepfakes”) that imitate, misrepresent, or harm any member of the school community – even if created outside school time.

#### Use of Devices and Software

- I will only use devices that meet the school’s BYOD specification (Windows-based laptop or MacBook).
- I understand that tablets and iPads are not permitted for BYOD use in school.
- I will install Microsoft Office 365 using my school account and keep my device updated and ready to use each day.
- I will not play games, stream content, or use social media on my device during school hours.

#### Security and Safety

- I will keep my passwords safe and not share them with anyone.
- I will not use VPNs, proxies, or apps that bypass school filters.

- I will report any misuse or concerning content to a teacher immediately.
- I will not attempt to access inappropriate websites or content.

### **Academic Integrity and AI**

- I will do my own work and give credit when I use information or support from others.
- I will only use AI tools when allowed by my teacher.
- I understand that copying or submitting AI-generated work without permission is not allowed.
- I understand that using AI to create fake or manipulated content about staff, students, or others (including images, video, or voice imitation) is strictly prohibited and may be treated as a safeguarding matter.
- I will follow the [School Name] AI guidance which explains when and how AI can be used responsibly to support learning – not replace it.

### **Photos, Videos and Online Sharing**

- I will not take photos or videos of others without their permission.
- I will not share content from school on social media or messaging apps.
- I will follow teacher instructions when asked to upload learning to platforms like Seesaw, Teams or other approved digital platforms.

### **Mobile Phones and Smartwatches**

- I will keep my phone in my locked Fixby Pouch throughout the school day.
- I will not access my phone until the end of the school day unless given permission.
- If I wear a smartwatch, I will ensure notifications and calling features are turned off.

### **Consequences and Monitoring**

- I understand that if I misuse digital technology or break this agreement, my access may be restricted.
- Devices may be checked by school staff if there is a safeguarding or behavioural concern (with parental consent).
- Repeated misuse may result in contact with my parents/carers and further consequences.

## Student Agreement

**By agreeing to these terms, I understand my responsibilities and agree to use technology safely, respectfully, and for learning.**

## Section 2 – Staff

### Professional Conduct & Digital Responsibility

- All staff are expected to model appropriate digital behaviour in line with Taaleem and school policies.
- Staff communications via email, Seesaw, Teams, and other platforms must reflect professional standards and uphold student safety and confidentiality.
- Staff must treat all personal data with care and follow school data protection procedures.
- Staff should model best practices for students by using technology purposefully and professionally. This includes limiting personal phone use during the school day.

### Device Use and BYOD

- All devices (school-owned and personal) must be used responsibly on the school network.
- BYOD devices must follow the guidance in the school's Device Usage and BYOD Policies.
- Staff may not connect unauthorised or unsecured devices to the network.
- VPNs or software that bypass filtering or security protocols are not permitted.

### Safeguarding and Online Safety:

- Staff must actively supervise students during device use and promote positive digital citizenship.
- Staff must immediately report any safeguarding concern, online misconduct, or inappropriate digital behaviour to the DSL through CPOMS.
- Photos, videos, and other media of students must only ever be captured on school-authorized devices.
- Personal mobile phones must not be used to capture, store, or share student content under any circumstances.
- Media must be stored in line with school protocols.

### Use of AI and Digital Tools:

- Generative AI tools (e.g. ChatGPT, Canva AI, Magic School) may be used to support planning, marking, and differentiation when used transparently and professionally.

- AI should not replace pedagogical decision-making or professional judgement.
- Staff must ensure student use of AI tools is age-appropriate, safe, and guided by clear boundaries.
- Please refer to the AI Policy for comprehensive guidance on AI use.

### Use of School Systems

- Staff must not share login credentials or allow others to access school systems using their accounts.
- Communication with students must only occur through official school platforms (e.g. Teams, Seesaw, school email).
- All school files must be stored using school-approved cloud services (e.g. OneDrive) to ensure data security.

### Social Media and Personal Devices

- Personal mobile phones must not be used to communicate with students or capture student data or images.
- Staff may not post school-related content on personal social media accounts without prior approval.
- All online interactions should protect the reputation of the school and comply with Taaleem's Social Media Policy.

### Monitoring and Compliance

- The school reserves the right to monitor usage of all school platforms and systems.
- Any breach of this AUP may result in disciplinary action in line with Taaleem HR procedures.
- Staff are expected to report technical issues or potential breaches promptly to the IT team or Senior Leadership.

## Section 3 – Guests

### Guidelines for Use

- Access is temporary and intended for professional or educational purposes only.
- Devices connected must be secured (e.g. passcode protected, free from malware).
- VPNs, proxies, or other tools used to bypass filters or monitoring are strictly prohibited.
- Streaming, gaming, or bandwidth-heavy activities that interfere with school operations are not permitted.
- Visitors must not access, view, or share inappropriate, offensive, or harmful content.

### Safeguarding and Privacy

- Guests must not record, photograph, or film students or staff without prior authorisation.
- Any digital interaction with students must be supervised and pre-approved by school staff.
- Guests may not access or attempt to access school systems, files, or cloud platforms.

### Monitoring and Compliance

- All activity on the guest network is subject to monitoring in line with school safeguarding protocols.
- Any misuse or breach of this agreement may result in immediate loss of access and further action if required.

### Guest Acknowledgement

By connecting to the [School Name] Guest Wi-Fi network, I confirm that:

- I have read and understood the terms outlined in this Acceptable Use Agreement.
- I agree to use the internet connection responsibly, professionally, and in line with [School Name]'s safeguarding expectations.
- I understand that any misuse may result in loss of access or further action.

## Version Control

| Version No. | Date        | Details of Changes                                                                                             |
|-------------|-------------|----------------------------------------------------------------------------------------------------------------|
| 1           | August 2023 | New policy                                                                                                     |
| 2           | August 2026 | Revamped in line with Compliance department’s guidance, updated processes and evolving regulatory requirements |
|             |             |                                                                                                                |
|             |             |                                                                                                                |

## Disclaimer

This document and its contents are the confidential and proprietary information of Taaleem Holdings PJSC and its subsidiaries. Any unauthorised access, distribution, or reproduction of this document is strictly prohibited.