Naas Academy

From: ***Naas Academy***
To: ***Respected Students and Parents***

Dear Students and Parents,

At NaaS Academy, we are deeply committed to fostering a safe, respectful, and inclusive digital learning environment for all. As part of our ongoing efforts to protect our students and promote responsible online behavior, we would like to inform you about our Anti-Cyberbullying Policy.

Please note that this policy is subject to annual review and revision to ensure it remains effective, relevant, and aligned with current digital safety standards. In cases where immediate concerns arise or significant adjustments are required, changes may be implemented during the academic year. Any updates to the policy will be promptly uploaded to our official website and communicated through appropriate channels.

We appreciate your continued support in upholding the values of kindness, accountability, and mutual respect within our community.

Warm regards,
Naas Academy Administration

--------------------*

Anti-Cyberbullying Policy

Empowering Safe, Respectful, and Responsible Online Learning

1. Purpose and Objectives

Naas Academy is committed to ensuring a safe and respectful digital learning environment for all students, staff, and parents. As a fully AI-powered online institution, we recognize the unique challenges and risks associated with cyberbullying. This policy aims to:

- Safeguard students and staff in the digital learning space.
- Educate all members of the school community about cyberbullying, its forms, and consequences.
- Establish clear procedures to prevent, identify, and address cyberbullying incidents.
- Encourage a culture of openness, safety, and proactive reporting.
- Evaluate and improve anti-cyberbullying strategies regularly.

2. What is Cyberbullying?

Cyberbullying refers to **intentional and repeated harm inflicted through digital means**, including messages, posts, or content shared via mobile devices, computers, or social media platforms.

Key characteristics include:

- **Deliberate behavior**: It is intentional, not accidental.
- **Repetition**: It occurs more than once over time.
- **Harmful impact**: It causes emotional or psychological distress.
- **Digital nature**: It uses devices or platforms such as messaging apps, social media, emails, or online forums.

Cyberbullying may include:

- Threats and intimidation
- Online harassment or stalking
- Defamation, ridicule, or spreading false rumors
- Impersonation
- Exclusion or group rejection
- Unauthorised sharing of private information or media
- Manipulation of digital content

3. Preventing Cyberbullying at Naas Academy

Education & Awareness

- Students and parents will be introduced to digital safety practices through our **AI Tutor modules**, PSHE sessions, and onboarding orientations.
- All students and parents are required to sign the **Safe and Acceptable Use Agreement (SAUA)** before accessing the Naas LMS.
- Cyber safety and respectful digital conduct will be integrated across subjects and reinforced through:

    - Live sessions
    - Online workshops and assemblies
    - Anti-Bullying Awareness Week
    - Student-led projects and discussions via the Virtual Student Council

Training for Staff

- Facilitators and staff undergo regular **e-safety training** to recognize signs of cyberbullying and handle incidents appropriately.
- Staff are trained to monitor LMS behavior flags and AI-triggered alerts that identify unusual or harmful patterns of student interaction.

4. Use of Technology and Online Conduct

Naas Academy actively promotes the **positive and responsible use of digital platforms**. Our systems are designed with safeguards including:

- Secure login systems with password policies
- Real-time AI monitoring of chatrooms, comments, and submissions
- Filtered communication channels within the LMS
- Timely reporting tools for students to flag incidents directly to staff

5. Reporting Cyberbullying

To ensure that students feel safe to speak up:

- Cyberbullying can be reported anonymously through the LMS or via email to designated staff.
- Students are encouraged to **preserve digital evidence** (screenshots, messages, posts).
- All reports will be treated confidentially and investigated swiftly.
- Staff are trained to identify non-verbal signs of distress or digital withdrawal.

6. Responding to Cyberbullying

While cyberbullying will be addressed under Naas Academy's broader **Anti-Bullying Policy**, specific responses to digital incidents may include:

Support for the Target

- Provide emotional reassurance and a supportive environment.
- Encourage the student **not to retaliate**, but to document the incident and inform an adult.
- Guide the student in adjusting privacy settings and blocking users if appropriate.
- Assist in reporting abusive content to platforms for removal.

Intervention with the Offender

- Help the student understand the impact of their actions.
- Apply appropriate disciplinary measures in line with Naas Academy's **Behavior Policy**.
- Involve parents or guardians as necessary.
- Require digital citizenship retraining or restorative justice dialogue (facilitated virtually).

Involving External Authorities

- If behavior violates laws (e.g., cyberstalking, hate speech, or threats), Naas Academy will involve legal authorities or internet service providers.

7. Parent and Student Engagement

- Parents will receive regular updates and resources on e-safety and cyberbullying awareness.
- The Virtual Parent Portal includes guides, reporting options, and tips for monitoring online activity at home.
- The Student Council will be actively involved in shaping digital safety initiatives and advising on improvements.

8. Monitoring and Policy Review

- All cyberbullying incidents will be **logged securely** and reviewed by the **Pastoral Care and Safeguarding Team**.
- The policy and prevention measures will be **reviewed annually**, incorporating feedback from students, parents, and staff.
- Data from the LMS and AI reports will inform continuous improvement efforts.

9. Policy Statement

Naas Academy promotes a culture of **digital respect, empathy, and accountability**. Cyberbullying in any form will not be tolerated and will be addressed with compassion, diligence, and firmness to protect the mental well-being of all students and staff.

<u>Cyberbullying: Investigation & Response Policy</u>

1. Investigation Protocol

At Naas Academy, **the safety and well-being of our students is our highest priority**. All reports of cyberbullying will be thoroughly investigated in accordance with our **Safeguarding and Child Protection Policy**. Investigations will be guided by the principles of fairness, confidentiality, and the protection of all parties involved.

Investigation Steps:

- Any staff member who receives a cyberbullying complaint must report it directly to the **Designated Safeguarding Lead (DSL)** or assigned **Student Welfare Coordinator**.
- All non-child-protection cyberbullying incidents will be **formally logged** and overseen by the **Head of Student Affairs**.
- Investigations will include **private interviews**, conducted virtually or via LMS conferencing tools, and will follow the **Naas Academy Anti-Bullying Framework**.
- Students and staff will be encouraged to **preserve all digital evidence**, including:
    - Screenshots of messages or posts
    - Saved emails or instant message logs
    - URLs and social media links
    - Copies of shared images or media
- If inappropriate or explicit images are involved, the content will be immediately referred to the **Senior Leadership Team (SLT)** and, where applicable, law enforcement authorities.
- In cases involving staff, complaints will follow our internal procedures in line with **child protection and safeguarding standards**.
- Devices may be **digitally quarantined or access revoked** temporarily during investigations, if deemed necessary.

2. Identifying the Offender

Identifying the source of cyberbullying may involve the following:

- **Internal LMS Monitoring**: Review of login logs, IP addresses, and activity records.
- **Witness Interviews**: Other students or participants may be able to confirm the source of abuse.
- **External Sources**: If the abuse originated on social media or mobile apps, platform providers may be contacted to block the perpetrator or remove harmful content.
- **Mobile & Network Tracing**: In severe cases, if bullying is done through withheld numbers or anonymous accounts, date/time logs will be gathered and the case may be referred to **cybercrime or law enforcement units**.

    While anonymity may make identification difficult, digital footprints often provide leads. However, impersonation, account hacking, or device sharing can complicate accurate tracing.

3. Sanctions and Disciplinary Action

Sanctions will be applied by the **Head of School** or **Head of Department**, depending on the nature and severity of the incident.

Objectives of Sanctions:

- Restore the victim's **sense of safety and security**.
- Hold the offender **accountable**, helping them recognize the harm caused.
- Send a clear message that **cyberbullying is unacceptable** and will not be tolerated.
- Support the perpetrator's **growth and behavior correction** through structured intervention.

Possible Sanctions May Include:

- Formal warning and parental notification
- Restricted access to LMS or communication tools
- Mandatory participation in digital citizenship or restorative learning sessions
- Removal of harmful content (by the student, or forcibly)
- Temporary or permanent suspension from classes or forums
- Referral to legal authorities (if behavior constitutes criminal conduct)

Important Considerations:

- Intent and impact will both be assessed.
- Retaliatory or unintentional actions will be evaluated contextually.
- Sanctions will be paired with **empathy-building and digital behavior coaching**.

4. Legal Considerations

Although cyberbullying is not always a clearly defined criminal offense, related acts may breach **cyber harassment, stalking, data misuse, and communication laws**.

Potentially Criminal Acts May Include:

- Harassment or cyberstalking
- Threats of violence or harm
- Unauthorised sharing of explicit images
- Defamation or incitement

Where a **criminal offense is suspected**, Naas Academy will **cooperate fully with legal authorities**, including:

- Handing over LMS activity logs
- Providing device or platform evidence
- Supporting students or families in filing formal complaints

5. Supporting All Parties Involved

For the Victim:

- Immediate emotional support and reassurance
- Guidance on protecting online privacy and removing harmful content
- Clear plan for ongoing monitoring and protection
- Involvement of the student's family, if appropriate

For the Perpetrator:

- Opportunities for reflection and behavioral reform
- Understanding of the consequences of their actions
- Accountability sessions and digital responsibility training
- Monitoring and follow-up to prevent recurrence

6. Monitoring and Review

- All investigations and outcomes will be documented in the **Digital Safety Incident Log**.
- Annual review of cyberbullying trends and procedures will be conducted.
- **Student and parent feedback** via LMS surveys and Virtual Council meetings will inform updates.

Note for Parents & Teachers at Naas Academy

- All staff are trained in **digital safeguarding** and regularly updated on cyberbullying trends.
- Parents can request support or report concerns via the **Parent Portal** or LMS messaging system.
- Students can also access in-platform safety tips via the AI Tutor dashboard.

Digital Safety & Cyberbullying Guidance

Recommended Resource: "Adolescent Volcanoes"

Adolescent Volcanoes is a highly effective book with dedicated sections for both teens and adults. It offers engaging exercises and activities to help adolescents:

- Understand and manage anger
- Establish healthy boundaries
- Communicate respectfully and assertively

It is a valuable resource for parents, educators, and young people themselves.

Online Safety: General Guidelines

At Naas Academy, we are committed to equipping our students and their families with the tools needed to stay safe online. To reduce the risk of exposure to inappropriate or illegal content and protect your privacy in the digital world, we recommend the following:

Protect Your Personal Information

- Never share your **full name**, **photos**, **email**, **phone number**, **location**, or **school name** online unless absolutely necessary and only with trusted sources.
- Avoid posting identifying information on **forums, gaming platforms**, or **public social profiles**.

Avoid Meeting Strangers

- Do **not arrange to meet** anyone you've only spoken to online. Always verify and involve a trusted adult if necessary.
- Online identities can be **fake**. Stay cautious, even if someone seems friendly or familiar.

Practice Safe Communication

- Do not open **emails, messages, or links** from unknown contacts.
- Avoid downloading **attachments or images** from unfamiliar sources—these may contain malware or offensive material.

Use Filtering and Parental Controls

- Activate **safe search settings** on search engines like Google, Bing, and YouTube.
- Regularly check and **reset filtering preferences**, as some systems may revert to unfiltered content.
- Use **parental control software** to monitor access to content and time spent online.

Viewing or sharing **illegal content**—especially involving child abuse or exploitation—is a **serious crime**. Report anything suspicious immediately through proper channels.

How to Handle Cyberbullying

Cyberbullying can affect anyone, and due to the anonymous nature of the internet, it may feel overwhelming. Below are essential strategies for students and families:

Think First, Act Smart

- **Talk to someone you trust** if you feel threatened or bullied online—this could be a parent, teacher, or counselor.

- **Never send bullying or threatening messages**—even jokingly.

Save and Document

- Keep **screenshots**, **emails**, **texts**, or **chat logs** of bullying behavior.
- Note the **date**, **time**, and **platform** the incident occurred on.
- If available, record any usernames or profiles involved.

Do Not Engage

- Do **not reply** to harassing or offensive messages.
- Responding may **escalate the situation** or confirm to the bully that you're affected.

Use Blocking and Reporting Features

- **Block** the person responsible via social media, messaging apps, or email.
- Report the behavior to the platform (Facebook, Instagram, WhatsApp, etc.).
- On Naas Academy's LMS, report directly via the "Report Abuse" or "Contact Admin" options.

Protect Your Account

- **Never share passwords** with anyone—even friends.
- Regularly update passwords and use **two-factor authentication (2FA)** when available.

Understand the Legal Implications

- Sending **abusive, threatening, or explicit messages** is a criminal offense.
- Sharing inappropriate images—even by forwarding—may result in **legal action**.
- **Bystanders have a responsibility** too: if you witness cyberbullying, **report it**. Remaining silent may be interpreted as complicity.

Naas Academy's Role in Online Safety

- Our **AI-driven LMS** uses time-tracking, chat filters, and safety alerts to detect unusual or concerning behavior.
- Students receive regular **digital citizenship education** through tutorials, assemblies, and campaigns like **Safer Internet Week**.
- We encourage open communication between **students, parents, facilitators, and our AI tutor, Dr. Naas**, to promote a safe, inclusive environment for all.
