INDIAN SCHOOL

RAS AL KHAIMAH

Cyberbullying Policy

This policy & procedures are reviewed annually to ensure compliance with current regulations.

	Approved/ Reviewed by
Policy Lead	Mr. Praveen P. P.
Role	Head of ICT
Date of Publication	05-04-2022
Date of first review	05-04-2023
Date of second review	05-04-2024
Date of third review	05-04-2025
Date of next review	06-04-2026
Signature	

Cyber bullying Policy

Rationale:

Indian School gives the technological advancement its careful attention for the benefit it has on students' lives, achievement, and career development. However, the school is mindful of the potential for bullying to occur. Central to the School's anti-bullying policy is the belief that 'all pupils have a right not to be bullied' and that 'bullying is always unacceptable'. The School alsorecognizes that it must 'take note of bullying perpetrated outside School which spills over into the School'. Based on this belief and on the UAE national restrictions set to terminate such types of bullying, the school has set this policy to protect all involved personnel.

Definition:

Cyberbullying may be defined as 'the use of electronic communication, particularly mobile phones and the internet, to bully a person, typically by sending messages of an intimidating or threatening nature: children and adults may be reluctant to admit to being the victims of cyberbullying'. It can take a number of different forms: threats and intimidation, harassment or 'cyber-stalking' (e.g. repeatedly sending unwanted texts or instant messages), sexting (e.g sending and receiving sexually explicit messages, primarily between mobile phones) vilification/defamation, exclusion/peer rejection, impersonation, unauthorized publication of private information/images and 'trolling' (abusing the internet to provoke or offend others online). It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, or humiliating material on websites, to include blogs, personalwebsites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to includeFacebook, YouTube and Rate my teacher

However it differs from other forms of bullying in several significant ways:

- by facilitating a far more extreme invasion of personal space. Cyberbullying can

take placeat any time and intrude into spaces that have previously been regarded as safe and personal.

- the potential for anonymity on the part of the bully. This can be extremely distressing forthe victim
- the potential for the bully to play very rapidly to a larger audience so the scale and scopeof cyberbullying can be greater than for other forms of bullying.
- through the knowledge that the data is in the world-wide domain, disproportionately amplifying the negative effect on the victim, even though the bully may feel his / heractual actions had been no worse than conventional forms of bullying

- the difficulty in controlling electronically circulated messages as more people get drawn inas accessories. By passing on a humiliating picture or message a bystander becomes an accessory to the bullying.
- the profile of the bully and target can be different to other forms of bullying as cyberbullying can take place between peers and across generations. Teachers can bevictims and age and size are not important.
- many cyberbullying incidents can themselves act as evidence so it is important the victimsaves the information. By cyber-bullying, we mean bullying by electronic media:

LEGAL ISSUES

Cyber-bullying is generally criminal in character. The law applies to cyberspace

- It is unlawful to spread defamatory information in any media including internet sitesCyber-bullying is a very serious concern that could cause irreparable psychological damage, especially to young people in their formative years.
- Schools are also being urged to help stop cyber-attacks by adopting an internet safety policyeducates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through ICT lessons and assemblies, continue to inform and educate its pupils in these fast-changing areas.

- IHS trains its staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it. It blocks access to inappropriate web sites, using firewalls, antivirus protection and filtering systems and no pupil is allowed to work on the internet in theComputer Room, or any other location within the school which may from time to time be usedfor such work, without a member of staff present. Where appropriate and responsible, IHS audits ICT communications and regularly reviews the security arrangements in place.

- Whilst education and guidance remain at the heart of what we do, the school reserves theright to take action against those who take part in cyber-bullying

. □ All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at alltimes. These acts may also be criminal acts.

- IHS supports victims and, when necessary, will work with the Police to detect those involvedin criminal acts.

- The school will use, as appropriate, the full range of sanctions to correct, punish or removepupils who bully fellow pupils or harass staff in this way, both in or out of school.

- IHS will use its power of confiscation where necessary to prevent pupils from committingcrimes or misusing equipment.

- All members of the School community are aware they have a duty to bring to the attention ofthe principal any example of cyber-bullying or harassment that they know about or suspect.

Preventing Cyberbullying

As with all forms of bullying the best way to deal with cyberbullying is to prevent it happening inthe first place. There is no single solution to the problem of cyberbullying but the school will do the following as a minimum to impose a comprehensive and effective prevention strategy:

Roles and

Responsibilities

Safeguarding Lead

The Principal who is also the Designated Safeguarding Lead will take overall responsibility forthe coordination and implementation of cyberbullying prevention and response strategies. The Principal will

- ensure that all incidents of cyberbullying both inside and outside school are dealt with immediately and will be managed and/or escalated in line with the procedures set out in the school's Anti-bullying Policy, Behaviour Policy and Safeguarding and Child Protection Policy.
- ensure that all policies relating to safeguarding, including cyberbullying are reviewed andupdated regularly
- ensure that all staff know that they need to report any issues concerning

cyberbullying to theSafeguarding Lead.

- ensure that all staff are aware of the Prevent Duties.
- provide training (using Channel online awareness training module) so that staff feel confident to

identify children at risk of being drawn into terrorism, to challenge extremist ideas and to knowhow to make a referral when a child is at risk. The Deputy Head is also the Designated Prevent Lead.

- ensure that parents/carers are informed and attention is drawn annually to the cyberbullying policy so that they are fully aware of the school's responsibility relating to safeguarding pupils and their welfare. The Cyberbullying Policy is available at all times on the school website
- ensure that at the beginning of each term, cyberbullying is revisited as part of the

Staying SafeProgramme and that pupils know how to report a concern

- ensure that all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology within school and beyond. All staff should sign to say they have read andunderstood the Staff Code of Conduct.

IT Head

IT Head will

- ensure that all pupils are given clear guidance on the use of technology safely and

positively both inschool and beyond including how to manage their personal data and how to report abuse and bullyingonline.

- provide annual training for parents/carers on online safety and the positive use of technology

- ensure the school's Acceptable Use Policy, Guidelines for Staff when Children are using DigitalDevices, Children's Use of Digital Devices and are reviewed annually

- provide annual training for staff on the above policies and procedures

- provide annual training for staff on online safety
- plan and deliver a curriculum on online safety in computing lessons which builds resilience in pupilsto protect themselves and others online.

- plan a curriculum and support PSHE staff in delivering a curriculum on online safety which buildsresilience in pupils to protect themselves and others online.

The IT Support and Development Manager will

- ensure adequate safeguards are in place to filter and monitor inappropriate

content and alert theSafeguarding Lead to safeguarding issues. The school uses a

third-party desktop lab solution

to filter all internet access. The internet filter records access to prohibited sites which

enables the ITSupport and Development Manager to report issues immediately to the

Designated Safeguarding Lead.

- ensure that visitors to the school are given clear guidance on the use of technology in school. This includes how to report any safeguarding issues to the Safeguarding Lead. Visitors will be given highly restricted guest accounts which will not allow any access to personal data and thatany misuse of the system will result in access to the system being withdrawn.

Guidance for Staff

Guidance on safe practice in the use of electronic communications and storage of images is containedin the Code of Conduct. The school will deal with inappropriate use of technology in line with the Code of Conduct which could result in disciplinary procedures.

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone
- Note clearly everything on the screen relating to an inappropriate text message or image, toinclude the date, time and names
- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image
- Inform the Deputy Head and Designated Safeguarding Lead immediately and pass them theinformation that you have

Computers

- Ask the pupil to get up on-screen the material in question
- Ask the pupil to save the material
- Print off the offending material straight away
- Make sure you have got all pages in the right order and that there are no omissions
- Inform a member of the Senior Leadership team and pass them the information that you have
- Normal procedures to interview pupils and to take statements will then be followed particularlyif a child protection issue is presented.

Use of Technology in School

All members of the school community are expected to take responsibility for using technologypositively.

As well as training, the following is in place:

- All staff are expected to sign to confirm they have read and understood the Acceptable UsePolicy.
- All staff are expected to sign to confirm they have read and understood the Staff Code ofConduct
- All staff are expected to have read and understood Guidelines for Staff when Children are usingDigital Devices
- All children are expected to have been taken through and understood Children's Use of DigitalDevices

Guidance for Pupils

If you believe you or someone else is the victim of cyber-bullying, you must speak to

an adult as soonas possible. This person could be a parent/guardian, or a member of staff on your safety network. For more advice, look at the Cyberbullying leaflet.

- Do not answer abusive messages but save them and report them
- Do not delete anything until it has been shown to your parents/carers or a member of staff atschool (even if it is upsetting, the material is important evidence which may need to be usedlater as proof of cyber-bullying)
- Do not give out personal details or contact information without the permission of aparent/guardian (personal data)
- Be careful who you allow to become a friend online and think about what information you wantthem to see.
- Protect your password. Do not share it with anyone else and change it regularly
- Always log off from the computer when you have finished or if you leave the computer for anyreason.
- Always put the privacy filters on to the sites you use. If you are not sure how to do this, ask ateacher or your parents.
- Never reply to abusive e-mails
- Never reply to someone you do not know
- Always stay in public areas in chat rooms
- The school will deal with cyberbullying in the same way as other bullying. Do not think thatbecause it is online it is different to other forms of bullying.
- The school will deal with inappropriate use of technology in the same way as other types of

  inappropriate behaviour and sanctions will be given in line with the school's Behaviour Policy.

Guidance for Parents/Carers

It is vital that parents/carers and the school work together to ensure that all pupils are aware of theserious consequences of getting involved in anything that might be seen to be cyber-bullying.
Parents/carers must play their role and take responsibility for monitoring their child's online life.

- Parents/carers can help by making sure their child understands the school's policy and, aboveall, how seriously the school takes incidents of cyber-bullying.
- Parents/carers should also explain to their children legal issues relating to cyber-bullying.
- If parents/carers believe their child is the victim of cyber-bullying, they should

save the offending material (if need be by saving the offensive text on their computer or on their child'smobile phone) and make sure they have all relevant information before deleting anything.

- Parents/carers should contact the school as soon as possible.If the incident falls in the holidays the school reserves the right to take action against bullying perpetrated outside the school bothin and out of term time.
- Parents/carers should attend the school's annual training on online safety delivered by the Headof Computing.

Consequences for Cyberbullies

The following consequences will be applied progressively based on the severity and repetition of cyberbullying incidents:

1. **Warning and Counselling:** For first-time or minor offenses, the student will receive a warning and mandatory counselling sessions to address the behaviour and its impact.
2. **Parental Involvement:** Parents/guardians will be notified and involved in meetings to discuss the incident and collaborate on behaviour improvement strategies.
3. **Behavioural Contract:** The student may be required to sign a behavioural contract outlining expected behaviour changes and consequences for further incidents.
4. **Detention:** The student may be assigned detention during breaks or after school hours.
5. **Loss of Privileges:** Temporary loss of school privileges, such as participation in extracurricular activities, access to school technology, or involvement in school events.
6. **In-School Suspension:** The student may be placed in in-school suspension, where they will complete their work in a supervised setting away from their peers.
7. **Out-of-School Suspension:** For severe or repeated incidents, the student may be suspended from school for a specified period.
8. **Expulsion:** In extreme cases, or if previous interventions have failed, the student may face expulsion from the school.
9. **Legal Action:** In cases where cyberbullying constitutes a criminal offense, the school may report the incident to the appropriate legal authorities.

The school will ensure parents/carers are informed of the cyber-bullying policy and the procedures inplace in the Anti-Bullying Policy to deal with all forms of bullying including cyber-bullying.

E-Safety at Home

Several sites offer helpful advice to parents/carers, particularly with respect to how they can bestmonitor their child's use of the computer at home. Here are some parents/carers might like to try:

www.thinkuknow.co.uk/parents

www.saferinternet.org.uk

www.childnet.com

Approved

Principal:

Chairman