ICS Policy Document

Whilst all Policies have a minimum date for review as a guideline, policies are under constant review. Changes to policies will occur as required.

Cyber Bullying Policy

Approved by: Principal Committee	Date: May 2020
Last reviewed on:	Date: N/A
Next review due by: 2 yearly	Date: May 2022

ICS recognises that a bullying incident should be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant harm.

Cyberbullying

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, unauthorised 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.

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 place at 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 for the victim.
- the potential for the bully to play very rapidly to a larger audience so the scale and scope of 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 / her actual actions had been no worse than conventional forms of bullying.
- the difficulty in controlling electronically circulated messages as more people get drawn in as 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 be victims and age and size are not important.
- many cyberbullying incidents can themselves act as evidence so it is important the victim saves the information.

Cyberbullying and the Law

Bullying is never acceptable and ICS fully recognizes its duty to protect all of its members and to provide a safe, healthy environment for everyone.

This policy is written in conjunction with the legislation identified at the end of this policy.

Preventing Cyberbullying

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

Roles and Responsibilities

The Principal who is also a Named Child Protection Officer (CPO) will take overall responsibility for the 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 Child Protection

Policy, and procedures Allegations against a Child and Allegations against a Staff Member.

- ensure that all policies relating to Child Protection, including cyberbullying are reviewed and updated regularly ensure that all staff know that they need to report any issues concerning cyberbullying to a Named Child Protection Officer.
- 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 protecting 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 student safety 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 and understood the Staff Code of Conduct.

The Head of ICT will:

- ensure that all pupils are given clear guidance on the use of technology safely and positively both in school and beyond including how to manage their personal data and how to report abuse and bullying online.
- 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 Digital Devices, Mobile Phone and Social Media policy 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 pupils to protect themselves and others online.
- plan a curriculum and support PSHEE staff in delivering a curriculum on online safety which builds resilience in pupils to protect themselves and others online.

The IT Manager will:

- ensure adequate safeguards are in place to filter and monitor inappropriate content and alert CPO's to child protection issues. The school uses a third party web-proxy solution to filter all internet access. The internet filter records access to prohibited sites which enables the IT Manager to report issues immediately to a Named CPO.
- ensure that visitors to the school are given clear guidance on the use of technology in school. This includes how to report any child protection concerns to the CPO's. Visitors will be given highly restricted guest accounts which will not allow any

access to personal data and that any misuse of the system will result in access to the system being withdrawn.

The Principals will

- ensure the school manages personal data in line with statutory requirements. The school is aware of its duties and follows our Data Protection policy.
- Careful consideration will be given when processing personal information so that the individual's privacy is respected where it needs protection. Access to the personal information will only be given to those who need it. The principles of the Data Protection Policy will be applied when processing, collecting, disclosing, retaining or disposing of information relating to a student or member of staff.

Guidance for Staff

Guidance on safe practice in the use of electronic communications and storage of images is contained in 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 student to show you the mobile phone
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names
- Make a transcript of a spoken message, again record date, times and names
- Tell the student to save the message/image
- Inform a Named CPO immediately and pass them the information that you have

Computers

- Ask the student to get up on-screen the material in question
- Ask the student 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 students and to take statements will then be followed particularly if a child protection issue is presented.

Use of Technology in School

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

As well as training, the following is in place:

- All staff are expected to sign to confirm they have read and understood the Acceptable Use Policy.
- All staff are expected to sign to confirm they have read and understood the Staff Code of Conduct

Guidance for Students

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or a member of staff on your safety network.

- 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 at school (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying)
- Do not give out personal details or contact information without the permission of a parent/guardian (personal data)
- Be careful who you allow to become a friend online and think about what information you want them 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 any reason.
- Always put the privacy filters on to the sites you use. If you are not sure how to do this, ask a teacher or your parents.
- Never reply to abusive emails
- Never reply to someone you do not know
- Always stay in public areas in chat rooms
- ICS will deal with cyberbullying in the same way as other bullying. Do not think that because it is online it is different to other forms of bullying.
- ICS 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 ICS's Behaviour Policy.

Guidance for Parents/Carers

It is vital that parents/carers and ICS work together to ensure that all students are aware of the serious 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 ICS's policy and, above all, how seriously ICS 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's mobile 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 ICS reserves the right to take action against bullying perpetrated outside the school both in and out of term time.
- Parents/carers should attend the school's annual training on online safety delivered by the Head of ICT.
- ICS will ensure parents/carers are informed of the cyber-bullying policy and the procedures in place 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 best monitor their child's use of the computer at home.

ICS takes e-safety at home seriously and has developed information available on our website to support both parents and students.

The ICS Esafety guide, along with links to additional guides and supporting websites can be found.

Linked Policies:

- Acceptable Use of IT
- Allegations Made Against Another Child
- Allegations Made Against an Employee
- Anti-bullying

- Behaviour Code for Adults Working with Children
- Children at Risk of Abuse Procedure
- Child Protection
- Confidentiality
- Disciplinary Procedure
- Equal Opportunities
- E-safety and Acceptable Use
- E-safety agreement
- HR recruitment
- Mobile Phone
- School Personnel Code of Conduct
- Special Educational Needs (SEND)
- Whistle Blowing

This policy is written in conjunction with the following legislation:

- ADEK Policy and Guidance Manual (2014-2015)
    - Policy 2: Ethical Leadership, Corresponding to Article (4) of the Organising Regulations
    - Policy 3: Students Protection, Corresponding to Article (5) of the Organising Regulations
    - Policy 23: The Principal's Authorities, Corresponding to Article (28) of the Organising Regulations
    - Policy 30: Professional Code of Ethics, Corresponding to Article (35) of the Organising Regulations
    - Policy 35: Records, Corresponding to Article (40) of the Organising Regulations
    - Policy 36: School Reports, Corresponding to Article (41) of the Organising Regulations
    - Policy 40: Elements of the Curriculum: Corresponding to Article (45) of the Organising Regulations
    - Policy 65: Protection from Dangers of the Global Information Network (the Internet), Corresponding to Article (70) of the Organising Regulations
- Child Rights Law, 2016, Federal National Council, UAE
- Article 274 of the Penal Code Federal (3) of 1987, as amended
- UAE Federal Law 5 of 2012 on Combating Cybercrimes
- UAE Federal Law No. 12 of 2016 amending Federal Law No.5 of 2012 on Combating Cybercrimes
- Relevant Ministry of Interior guidance on protecting children from harm
- ADEK-MoI CPC Memorandum of Understanding of 2015
- Ministry of Interior – Child Protection Center website (www.moi-cpc.gov.ae)
- UN Convention on the Rights of the Child, 1989, ratified by the UAE 1996
- "Preventing and Tackling Bullying", DfE, July 2017, UK

- “Keeping Children Safe in Education” DfE statutory guidance, 2018
- ‘Sexual violence and sexual harassment between children in schools and colleges’, DfE, 2018, UK