ISCS E-SAFETY POLICY

مدرسة الإبداع العلمي الدولية
INTERNATIONAL SCHOOL OF CREATIVE SCIENCE

Created: April 2020

Next Review: September 2021

ISCS E-SAFETY POLICY

Contents

ISCS E-SAFETY POLICY

Introduction

At ISCS we are committed safeguarding our students through prevention, protection and support. We believe that everyone in the school community has the right to learn and to teach in a supportive and caring environment without the fear of being bullied.

We are committed to helping all members of the school community to benefit from information and communication technology, while understanding its risks, and to equip children with the knowledge and skills to be able to use it safely and responsibly.

The school recognises that any 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.

Purpose

This E-Safety policy enables our school to create a safe e-learning environment that:

- protects children from harm
- safeguards staff in their contact with pupils and their own use of the internet
- ensures the school fulfils its duty of care to pupils
- provides clear expectations for all on acceptable use of the internet.

Aims

- to use technology safely and respectfully
- to identify a range of ways to report concerns about content or contact
- to show how to keep personal information private
- to recognise acceptable/unacceptable behaviour

Managing Access

School Accounts

All ISCS students and users have an account on MS Office 365. All users must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.

Social Networking and Personal Publishing

- The school blocks access to social networking sites.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.

- School staff are advised not to add children, or parents as 'friends' if they use these sites.

Use of School e-mail

- Pupils must not send or attach documents containing offensive, threatening, derogatory, racist or sexually explicit material.
- Pupils must not send obscene, abusive or sexually explicit language.
- If any of the above is received by a user a teacher must be informed. Do not reply.
- Pupils must not harass other users. This includes: forwarding chain letters; deliberately flooding a user's mailbox; sending mail that is designed to interfere with the e-mail system.
- Pupils must not access, copy or transmit another pupils message or e-mail address without their permission.
- Pupils must not forge a message to make it appear to come from another person.

Purpose

As a school, it is our duty of care alongside that of staff/parents/carers and other members of the community to protect our children and young people from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this e-safety policy is to outline what measures we take to ensure that pupils can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate manner.

E-Safety Roles & Responsibilities

Our school will endeavour to ensure the e-safety of all its members. It will use education, technology, accountability and responsibility as the key ways to achieve this. Within our school, all members of staff and pupils are responsible for e-safety, responsibilities for each group include:

Students

Students are responsible for ensuring that:

- Behave responsibly and appropriately when using communication technology including the internet and online behaviour platforms.
- Student must follow the e-behavior policy.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- They know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying
- Do not respond to cyberbullying. Take evidence (pictures or print outs of emails, messages, pictures or videos sent).

Teaching Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They report any suspected misuse or problem to the Supervisors, Social worker or the Head of Section.
- All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use.

Supervisors

- Motivate students in displaying positive behaviour online.
- Issue all verbal and written warnings
- open a file when an offence is committed
- Inform parents when a warning is given
- Deduct the behaviour marks and record it.
- Coordinate with social workers on all behaviour cases.
- In absence of the supervisor, the social worker will take over the above responsibilities

IT Department

School IT department is responsible for ensuring that:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-safety officer/ Principal for investigation/action/sanction.

E-Safety/Computing Lead – Shajeda Begum

- Leads on e-safety issues
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Reports regularly to Principal Academic Team

Social workers

Social workers are responsible for ensuring that:

- They promote awareness on all forms of bullying for students, parents, and staff members.
- They run national anti-bullying week programme.
- They maintain and review anti-bullying and cyberbullying policy
- They bring cases to behaviour management committee/SMART learning teams
- They follow ISCS anti-bullying policies and MOE behaviour policy when dealing with e-safety/cyberbullying cases.
- They maintain records of each cyberbullying case

Parents

Parents are responsible for ensuring that:

- Children are monitored when they are online, especially during online learning phase.
- They are warned of the negative side of communication technology.
- Children are instructed to report any concerns to them or the school management.
- They help their child act with self-confidence.

Cyber Bullying

Cyberbullying is 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), (e.g sending and receiving 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.

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 the school will do the following as a minimum to impose a comprehensive and effective prevention strategy:

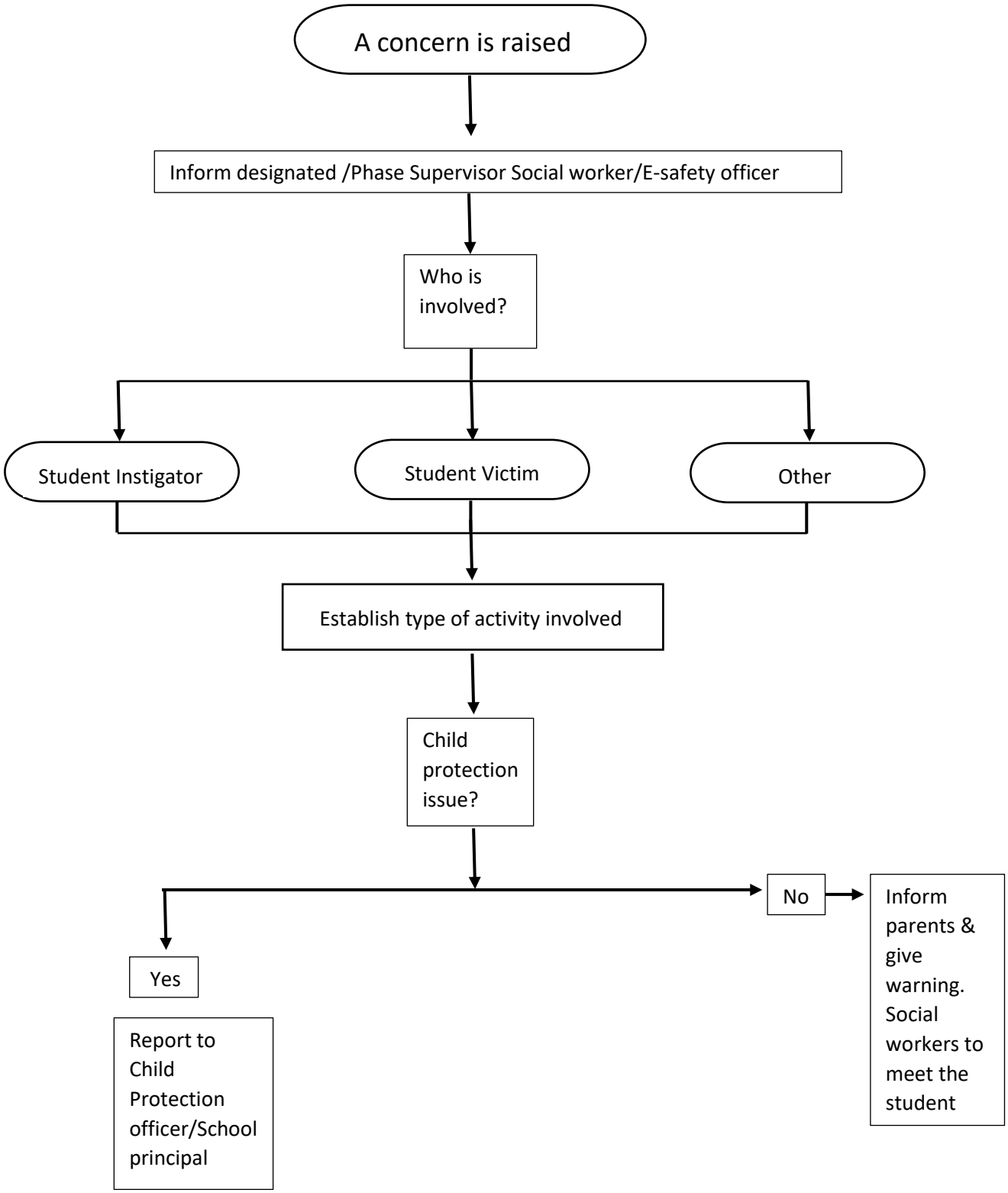
The Head of Computing will:

- 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, 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 pupils to protect themselves and others online.
- plan a curriculum and support staff in delivering a curriculum on online safety which builds resilience in pupils to protect themselves and others online.

Practices and Procedures

The school will encourage safe use of IT, emphasizing, for example, the importance of password security and the need to log out of accounts.

The school will promote the message that asking for help is the right thing to do. All members of the school community will refer to the flowchart below to report any e-safety concern/ cyberbullying.


A concern is raised
Inform designated /Phase Supervisor Social worker/E-safety officer
Who is involved?
Student Instigator
Student Victim
Other
Establish type of activity involved
Child protection issue?
No
Inform parents & give warning. Social workers to meet the student
Yes
Report to Child Protection officer/School principal

Investigation

The nature of any investigation will depend on the circumstances. The SMART learning team which consists of will consist of the Principal, the Academic Team, the Head of Section, Social Worker, and Teacher will be involved in all E-safety & cyberbullying cases. The investigation may include:

- A review of evidence and advice to preserve it, for example by saving or printing (e.g. phone messages, texts, emails, website pages, screenshots of online learning platforms).
- Efforts to identify the perpetrator, which may include looking at the media, systems and sites used.
- Speaking to witnesses who may have useful information.
- Requesting a student to reveal a message or other phone content or confiscating a phone (Staff do not have the authority to search the contents of a phone).

Working with the perpetrator

Work with the perpetrator and determine sanctions on an individual basis, with the intention of:

- Helping the person harmed to feel safe again and be assured that the bullying will stop
- Holding the perpetrator to account, so they recognise the harm caused and do not repeat the behaviour
- Helping bullies to recognise the consequences of their actions and facilitating change in their attitude and behaviour

Note: Always report bullying incidents. Not doing that allows the bully to continue. That's not good for the victims, for those who witness the incidents or for the bully, who may need help to change their antisocial behavior.

Technology Platforms

The teachers will use appropriate platforms for each year/grade level groups for effective distance learning. Some of the key platforms being used are:-

KG

1. Microsoft Office 365 Teams – to facilitate online (both synchronous and asynchronous) discussions, meetings and sharing of resources
2. Class Dojo - enables teachers to share content, distribute quizzes, assignments, and manage communication with students, colleagues, and parents

Lower Primary

1. Microsoft Office 365 Teams – to facilitate online (both synchronous and asynchronous) discussions, meetings and sharing of resources
2. Class Dojo - enables teachers to share content, distribute quizzes, assignments, and manage communication with students, colleagues, and parents
3. NearPod – Student engagement platform where teacher can create presentations that can contain quizzes, polls, videos, images, drawing-boards, web content and so on

Higher Primary

1. Class Dojo – enables teachers to share content, distribute quizzes, assignments, and manage communication with students, colleagues, and parents
2. Microsoft Office 365 Teams – to facilitate online (both synchronous and asynchronous) discussions, meetings and sharing of resources
3. NearPod – Student engagement platform where teacher can create presentations that can contain quizzes, polls, videos, images, drawing-boards, web content and so on

Secondary School

1. Microsoft Office 365 Teams – to facilitate online (both synchronous and asynchronous) discussions, meetings and sharing of resources
2. Subject online resources like Pearson Activelearn to help students to access the subject content
3. Google Classroom - enables teachers to share content, distribute quizzes, assignments, and manage communication with students.

Access to the network, to the internet and to e-mail

Access to these school facilities is regarded as a privilege and not a right. Access may be denied if a user breaches the conditions of use.

Course Requirement Users who depend on access to the school network for any requirement of any course could, by breaching the conditions of use, be responsible for their inability to complete a course requirement. This would have an obvious impact on the assessment of that course.

General Advice to users

1. Notify an adult immediately, if by accident, you encounter materials that violate this Acceptable Use Policy.
2. Be prepared to be held accountable for your actions and for the loss of privileges if you breach this Policy.
3. Do not share your password with another person.
4. Log out of the network whenever you leave a computer unattended.

Support

- Academic issues – Any academic issues should be firstly raised to the teacher/subject teacher. Should you require any further clarification, then please contact the HOS/HOD responsible for your child's year level.
- IT/Technical/E-Safety Issues – Please contact the IT personnel for any issues arising with log ins, software or other technical elements during the distance learning period, and Phase supervisors for E-Safety.

Related Policies

- ISCS Student Behaviour Management Policy for Distance Learning
- BEAM Acceptable Use Policy
- BEAM Cyber Security Policy