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.

Acceptable Use of I.T. Policy

Approved by: Governing Board	Date: November 2022
Last reviewed on:	Date: N/A
Next review due by: 2 years	Date: November 2024

Overview

This policy and the procedures that it underpins apply to all children and staff, including senior managers and the board of trustees, paid staff, volunteers, agency staff and anyone working on behalf of ICS.

- To protect children and young people who receive ICS's services and who make use of information technology (such as mobile phones, games consoles and the Internet) as part of their involvement with us.
- To provide staff and volunteers with the overarching principles that guide our
- approach to e-safety.
- To ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use information technology.

Any breach of this policy will lead to disciplinary action.

Aims

Ensure that students benefit from all learning opportunities offered by the computing and internet resources provided by the school in a safe and controlled manner.

- To give students clear guidance on safe and acceptable use of these resources.
- Make students aware that Internet use in school is a resource. If the resource is abused, then access will be denied.

At ICS we will develop the learning environment to provide a range of ICT opportunities and tools. This will empower our children to make relevant and safe choices and be flexible as they develop their personalised learning in line with our school's vision.

General

- Virus protection software is used and updated on a regular basis.
- The ICT Leader is the appointed member of staff responsible for e-safety.

Students' Access to the Internet

ICS use a 'filtered' Internet Service, which will minimise the chances of students encountering undesirable material. ICS will normally only allow children to use the Internet when there is a responsible adult present to supervise. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to students, the expectations we have of students.

Teachers will have access to students' screens and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.

Expectations of students using the Internet

- All students are expected to read and agree to the E-safety Agreement.
- At ICS, we expect all students to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.
- Students using the Internet are expected not to deliberately seek out offensive materials. Should any students encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Students are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.
- Students must ask permission before accessing the Internet.
  Students will not access social networking sites unless expressly permitted by the school or as part of a specific learning activity.
- Students should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No applications may be downloaded to the school's computers from the Internet or brought in on portable media from home for use in school
- School work completed at home may be brought in on portable media, but this must be virus scanned by the class teacher before use.

- Personal printing is not allowed on the school network.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- The school encourages the use of anti-virus software on machines used at home.
- Students consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

School Website

- The website will be regularly checked to ensure that there is no content that compromises the safety of students or staff.
- The publications of children's work will be decided by a teacher.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Photographs and videos focusing on individual children will not be published on the school website without parental permission.
- The school website will avoid publishing the full names of individuals in a photograph.
- The school will ensure that the image files are appropriately named and will not use students' names in image file names if published on the web.

Personal Devices

Students may only use their own technology in school as part of a pre-arranged educational activity, with permission from a member of staff and authorised by the ICT Leader.

Inappropriate use is in direct breach of ICS's Acceptable Use and Mobile Phone policy.

Sanctions

Persistent misuse of the internet by students will result in reduced access to the Internet.

Misuse of other technologies will result in a complete ban and/or confiscation. Both of these actions will take place for a set period of time agreed by the Principal. Parents will always be notified. No application or services accessed by students or their parents may be used to bring the school or its members into disrepute.

All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.

Linked Policies:

- Behaviour Code
- Child Protection
- E-safety

- E-safety agreement
- Mobile Phone Policy

This policy is written in conjunction with the following legislation:

- ADEK Policy and Guidance Manual (2014-2015)
  - Policy 3: Students Protection, Corresponding to Article (5) 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
- 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