1 Rationale:

The School recognizes that excellence in education requires that technology is seamlessly integrated throughout the educational program. Increasing access to technology is essential for that future. We also recognize that technology plays an important and positive role in everyone's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

Research into cyber bullying indicates that it is a feature of many young people's lives. Cyber bullying, like all

Other forms of bullying should be taken very seriously. It is never acceptable.

The policies, procedures and information within this document apply to all wireless mobile devices used at DHIS, including any other device considered by the Leadership Team to come under this policy.

2 Aims:

The aims of this policy are to ensure that:

- we safeguard the pupils in the real and virtual world
- students, staff and parents are educated to understand what cyber bullying is and what its consequences can be
- knowledge, policies and procedures are in place to prevent incidents of cyber bullying in school or within the school community
- we have effective measures to deal effectively with cases of cyber bullying
- we monitor the effectiveness of prevention measures

3 Definition of Cyber bullying:

Cyber bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others.

Cyber bullying can involve Social Networking Sites, emails and mobile phones used for SMS messages and as cameras. In addition;

- It can be used to carry out all the different types of bullying; an extension of face-to-face bullying
- It can also go further in that it can invade home/personal space and can involve a greater number of people
- It can take place across age groups and school staff and other adults can be targeted
- It can draw bystanders into being accessories
- It includes: threats and intimidation; harassment or 'cyber stalking'; vilification; exclusion or peer rejection; Impersonation; and manipulation
- It includes cyber stalking, e.g. repeatedly sending unwanted texts, defamation
- It includes the circulation of private information or images
- It can be an illegal act as in the UAE it is unlawful to disseminate defamatory information in any media

Including internet sites

4 Policy Procedure

Darul Huda Islamic School educates students both in the proper use of technology and about the serious consequences of cyber-bullying and will, through curriculum links, computing lessons and assemblies, continue to inform and educate its students in these fast-changing areas.

All students and teachers must sign the Acceptable Use of Technology Agreement.

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

Leaders know to respond effectively to reports of cyber-bullying or harassment and as a school there are systems in place to respond to it.

Darul Huda Islamic School endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems.

Students are only permitted to use devices connected to the internet with permission from a teacher.

Whilst education and guidance remain at the heart of what we do, Darul Huda Islamic School will take action against those who take part in cyber-bullying in line with the guidelines in the Anti-Bullying policy. In addition, DHIS will confiscate devices where necessary to prevent students from misusing equipment.

If an incident takes place in the evening or at the weekend, DHIS reserves the right to take action against bullying perpetrated outside the school which spills over into the school.

Darul Huda Islamic School will keep good records of all cyber bullying incidents on SIMS

Students are encouraged to report any suspicions of cyber bullying and have access to the school counsellor.

Support is offered to victims of cyber bullying including emotional support and reassurance.

Sanctions are issued in line with our Anti-Bullying policy.

5 Roles and

Responsibilities: Staff

All staff has a responsibility to prevent misuse of equipment and cyber bullying Staff may ask to look at content on a student's personal device, but it is good practice to do so with 2 adults present.

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 member of the Senior Leadership team and pass them the information that you have

Computers/Laptops/iPADS

- Ask the students to get up on-screen the material in question.
- > Ask the students to save the material.
- > If possible, Print off the offending material straight away.

- > If possible and with the student's agreement a screen capture image may be able to be sent to the staff's school email account
- > Inform a member of the Senior Leadership team and pass them the information that you have.

Normal anti-bullying procedures to interview students and to take statements will then be followed particularly if a child protection issue is presented.

Students:

- > Should follow the school's code of conduct / behaviour policy, when writing online. It is acceptable to disagree with someone else's opinions, however, do it in a respectful way. What is inappropriate in the classroom is inappropriate online.
- > Must speak to an adult as soon as possible if they believe someone is a victim on cyber bullying.
- ➤ Should not answer abusive messages but save them and report them
- > Should not delete anything until it has been shown to parents or a member of staff at DHIS(even if it is upsetting, the material is important evidence which may need to be used later as proof of cyberbullying)
- > Should not give out personal IT details
- > Should never reply to abusive e-mails or messages in chat rooms or other social media
- ➤ Should never reply to someone you do not know

Parents

- > It is vital that parents and the school 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 can help by making sure their child understands the school's policy and, above all, how seriously DHIS takes incidents of cyber-bullying
- > Parents should also explain to their children legal issues relating to cyber bullying
- > If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything
- > Parents should contact the school as soon as possible. A meeting can then be arranged with a member of the Senior Leadership Team

Approved for issue:

Mr. Muneer Chalil

Principal.

This Policy will be revised if any amendment is made by ADEC to the existing ADEC Unified Child protection policy and regulation 2020

Copy to:

- 1. Stock file.
- 2. Office of Principal/VP/Supervisors
- 3. School library
- 4. Staff room & School clinic
- 5. School website.

ICT POLICY

Objective

Darul Huda Islamic School aims to educate staff and students to use ICT effectively to support and develop their lifelong learning.

To use ICT as an effective and efficient teaching, learning, communication and management tool throughout the school.

- To continuously improve the ICT capability of students and staff.
- To provide access to high quality ICT resources and support for staff and students.

Whole-school issues

The school's policy is to use and develop the opportunities provided by ICT to benefit the entire school community.

IT Curriculum issues

Teaching staffs continue to review all teaching and learning in line with current ICT good practice.

A whole-school network supports curriculum delivery for all subject areas in providing networked resource materials, teacher-researched Internet links for student use and material for staff curriculum related professional development.

The network is maintained and developed by the IT Technician.

Student Issues

Students are facilitated with supervised use of ICT. Several departments also ensure that pupils have access to ICT in their subject area via a booking system of Computer Room and Language Room. It is important that ICT is used effectively to support access to the curriculum for all students. Identified students may have access to additional resources such as laptops with specific software to support curriculum access.

Staff issues

All members of staff are offered training to improve their ICT capability and have a responsibility to keep abreast of developments in ICT.

The IT Technician can be contacted to request additional support and training in the use of ICT.

There is continuous attention to improving the quality of staff computers throughout the school subject to budgetary control.

Network access

Staff and students have access to reliable and industry-standard hardware and software in order to use ICT effectively as a teaching and learning resource. It is also used as a working tool for management and administration.

Every classroom has at least one PC and Overhead projector for staff use.

All staff and student users have access through the school's network to their personal data areas and shared data.

All applications are held locally except for Internet.

Computers for staff/student use

Teaching of core ICT and ICT within subjects is mainly in the Computer Room and Language Room. "Free" slots are can then be booked in any of the rooms by any member of staff when needed.

A policy of integrating ICT into teaching and learning across the curriculum has been reflected in the provision of a PC and digital projector in all classrooms and also by providing teachers with ICT access outside the main ICT rooms and classrooms. Teachers have also been provided secure network access for personal laptops and use the same Anti-virus software as school provided equipment. This access is maintained by the IT Technician.

Technical Support

On-site technical support for the curriculum network is provided by the IT Technician who is responsible for the day-to-day maintenance of the network

infrastructure, all hardware and software owned by the school, and the provision of technical support for all ICT users.

The administrative network, Facility Administration, is supported by the IT Technician, with assistance of Office Staff.

The ICT inventory is incorporated within the schools asset records, and is updated every 6 months to show current locations, and other pertinent information for all ICT hardware.

Sustainability

Technical support routines and procedures are continuously reviewed and developed to ensure the sustainability of the network infrastructure, hardware and software.

The whole school asset register provides a continuously-updated audit of hardware that facilitates decisions on repair, replacement and development.

The whole school annual budgetary cycle provides the opportunity to identify maintenance, replacement and development needs for ICT infrastructure, network services, technical support, equipment and software. The "core" annual budgets are ICT General and Capital.

Before being disposed of, all ICT equipment is firstly made safe and removed from the schools register of assets. All hard drives are either destroyed or reformatted to wipe all data stored for possible reuse. Equipment is then stored in a secure location on site and then removed to the local recycling facility,

Emerging technologies

Teachers are encouraged to attend in-service on the use of ICT in the classroom.

If a development in (hardware or software) is deemed to have the potential to improve teaching and learning or administration it will be reviewed, trialled and, if proved to be successful, incorporated into whole school use depending on budgetary constraints.

Home-school links

Information about the school, including the newsletter, is made available to staff, students, parents/guardians and the general public on the school's website.

Parents/Guardians **are informed** if their child is found to be using the network or the internet in any way that contravenes the "Acceptable Use Agreement".

The school website is kept up to date by the IT Technician. All staff members are encouraged to inform her of any changes that need to be made.

Acceptable Use Agreement

The purpose of the Computer Resources policy is to provide a framework for the use of ICT by students and staff. The school has provided ICT equipment for use by students offering a vast amount of information and offering great potential to support the curriculum.

In this policy, computing resources are defined as those computers, computer software, networks, and electronic messaging systems (e-mail, voice mail, facsimile and imaging systems) operated by or for the benefit of the students of the school. The use of these resources is a privilege, not a right and inappropriate use will result in that privilege being withdrawn. It is the student's responsibility to use these resources in a manner that is efficient, ethical and legal.
