Dubai English Speaking School

Online Safety Policy

Written by	Andrea Harrow	**Updated:**	November 2022
Approved by	Tony Clarkson	**Review Date:**	November 2023

DESS Online Safety Policy

Dubai English Speaking School acknowledges the duty of care to safeguard and promote the digital welfare of children and is committed to ensuring that any incidences of online safety risks or concerns are appropriately addressed with immediate action.

The purpose of this policy is to safeguard and protect all members of our school online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture.

This policy is applicable to all members of Dubai English Speaking School; including staff, students and pupils, volunteers, parents/carers and visitors who have access to and are users of DESS's digital technology systems, both internally and externally.

At DESS we believe:
- Online safety is an essential element of safeguarding
- The internet and associated devices are an integral part of everyday life
- All learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks

At DESS we will:
- Uphold online safety as a safeguarding issue which is embedded across the whole school culture
- Incorporate the principles of online safety across all elements of school life
- Ensure that children are provided with a safe environment in which to learn and develop
- Proactively engage staff, pupils and parents in school activities that promote the agreed principles of online safety
- Ensure staff understand their roles and responsibilities regarding online safety
- Ensure that staff receive appropriate child protection training
- Enable staff to know how to recognise, respond to and report signs of online abuse and harm
- Ensure children are being appropriately taught about and know how to use the internet responsibly
- Ensure that children read and adhere to acceptable use policies
- Ensure that children engage in age-appropriate online safety education opportunities
- Promote online safety and the adoption of a whole school approach
- Ensure that the school has appropriate filters and monitoring systems in place
- Ensure children know how, when, and where to report concerns and when to seek help from a trusted adult

At DESS we recognise that:
- All children regardless of age, disability, gender, racial heritage, religious belief, or identity, have a right to equal protection from all types of harm or abuse.
- Working in partnership with children, their parents, carers and other agencies is essential in promoting children's welfare

At DESS we aim to:
- Protect all children and staff from potential online harm
- Raise awareness of online safety issues and equip children with the skills needed to keep them safe
- Ensure that all staff have read and understand the Online Safety Policy and know how to recognise, respond and report signs of online abuse
- Cultivate a safe, trusting environment in which children feel empowered to seek support if they are concerned or upset by something they have seen online.
- Share information about online safety with students, parents, and staff outside providers,

interns, volunteers and visitors.
- Model good practice when using technology

Responding to Online Safety Concerns
The safety of our children is of paramount importance. Any concern that a child may be at risk of harm or abuse must immediately be reported. The DESS Safeguarding and Child Protection Policy includes procedures to follow regarding online safety concerns. (see separate policy)

SEND and Children with Additional Vulnerabilities
DESS recognises that any learner can be vulnerable online, ant that their vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, such as those with special educational needs, who may be more susceptible to online harm or have less support from their families in staying safe online. We aim to ensure the effective and safe provision of tailored online safety education so that all learners receive the information and support they need.

Remote Learning (should DESS move back to this)
If DESS moved to Remote Learning the aims and purpose of the policy have not changed: all stakeholders need to be fully aware of all procedures to keep themselves safe and know the procedures for reporting concerns or incidents.

Additions:
- Online Live Learning Policy developed and shared to ensure safe use of 'live' sessions (see separate policy). This includes guidance for staff, parents and children.
- Online Live Learning Policy includes an appendix: DESS Online and Meeting Etiquette for Children (see separate document). This outlines the expectations for children during any live session undertaken during Remote Learning.

Role of SLT:
- To ensure all Remote Learning policies and procedures are being carried out and that any incidents are immediately reported to the Headteacher or DSL
- To approve any external links being shared with the children and ensure that all YouTube clips are shared through 'Pure View'

Role of teachers:
- To ensure all live sessions are carried out in a manner which safeguards themselves and the children
- To ensure they are fully aware of all policies relating to Remote Learning and regularly discuss these with the children
- Ensure the children are reminded of the expectations of them and of how they can keep themselves safe whilst online
- To ensure all external links shared with the children have been approved by SLT
- To ensure all YouTube links have been through 'Pure View' first to remove all adverts and suggested clips

Role of parents:
- To support the school in ensuring their children are safe online. To be aware of the policies and procedures relating to 'live' sessions
- To report any concerns to the school

Role of children:
- To ensure they follow the 'DESS Online and Meeting Etiquette for Children' at all times
- To ensure they know what to do if an online safety issue arises
- To know who they would contact if they do not feel safe when working online

NB: this policy should be read online side our safeguarding and child protection, and social media policies.

As an addendum to the Online Safety Policy, here are the types of online risk which usually fall under one of three categories:

Contact: Contact from someone online who may wish to bully or abuse the child. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting person information.

Content: Inappropriate material available to children online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.

Conduct: The child may be the perpetrator of activities including: illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

Defining online abuse:

"Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones" (NSPCC, 2019).

Hidden harms – types of online abuse may include:
- Cyberbullying
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:
- Neglect
- Sexual
- Physical
- Emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:
- harassment
- stalking
- threatening behaviour
- creating or sharing child sexual abuse material
- inciting a child to sexual activity
- sexual exploitation
- grooming
- sexual communication with a child
- causing a child to view images or watch videos of a sexual act.

At DESS, we teach the Digital Literacy strand of our Computing curriculum following the UKCCIS

'Education for a Connected World' framework, which aims to equip children and young people for digital life. It covers:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

E-Safety Incident Log

Number:	Reported By: *(staff name)*	Reported To: *(e.g. Head, e-Safety Officer)*
	When:	**When:**

Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)

Review Date:	

Result of Review:

Signature (Headteacher)		**Date:**	