



## **CYBER SAFETY & ANTI BULLYING POLICY**

*This policy is part of a series of interrelated policies for the safety and wellbeing of students, parents and staff.*

*This policy should be read in conjunction with the following policies:*

- *Sensitive Data Policy*
- *Data Protection Policy*
- *Acceptable use Policy*

### **PURPOSE OF POLICY**

- *Promote safe and responsible use of digital platforms and encourage positive interaction within the digital community.*
- *Educate students and parents on appropriate online behavior for educational purposes.*
- *Set expectations for student behavior when using digital technology, in line with school policies and procedures.*
- *Implement policies and procedures to prevent and address cyberbullying within the school community.*

### **AT DBS, STUDENTS ARE TAUGHT TO:**

- *Understand how to use technology safely and be aware of the risks and consequences of misuse.*
- *Know how to respond if they or someone they know is being cyberbullied.*
- *Report any issues related to cyberbullying and seek support from the school and parents to address the problem.*

### **STATEMENT OF POSITION:**

- *DBS ensures cyber-safety through core values, including rigorous cyber-safety practices and educational programs.*
- *The school provides appropriate use agreements for both staff and students, emphasizing responsibilities and obligations for safe use of ICT equipment.*
- *The goal is to create and maintain a cyber-safe culture aligned with the school's values and legal requirements.*

- *Students will receive an acceptable use policy, and after signed consent, they can access school ICT devices, with clear consequences for breaches related to cyber-safety and bullying.*

### **CYBER SAFETY**

- *Cyber safety covers technologies such as the Internet, mobile phones, and wireless devices.*
- *With advanced and affordable communication technologies, it is important to educate children and young people about the benefits and risks.*
- *It provides safeguards and awareness to help users manage their online experiences.*
- *Promotes the appropriate and responsible use of all technologies.*

### **GOOD HABITS:**

- *Cyber-safety relies on responsible ICT use by both staff and students, supported by education and clear policies.*
- *Effective implementation of cyber-safety policies in administration and curriculum, including secure network design, is essential.*
- *Safe and secure broadband usage, along with proper content filtering management, is crucial for cyber-safety.*

### **AT DBS:**

- *The school takes all reasonable steps to protect students online but acknowledges the risk of exposure to undesirable content.*
- *Students are regularly reminded to:*
- *Turn off the screen if they encounter inappropriate material.*
- *Report the issue immediately to a teacher or supervising adult, who will document the details.*
- *Refrain from describing or encouraging others to access the site.*
- *If unsuitable content is encountered on school platforms, both learners and teachers must contact the IT manager immediately.*

### **STEPS WE TAKE TO PROTECT OUR LEARNERS AT DBS**

- *Filtered Service: Internet access is provided through a filtered service on-site.*
- *Supervision: All children's internet use is supervised by a teacher, as no filtering service is 100% effective.*
- *Planned Activities: Internet use is planned and purpose-driven, not for aimless surfing. Children use the internet in response to specific class needs or questions.*
- *Websites: Teachers preview and revisit websites to ensure they meet curriculum needs and are age appropriate. Britannica search engine is used, and teachers guide students in using safe search terms.*

- *Internet Safety Rules: Children are taught Internet Safety Rules and encouraged to discuss how to handle encountering inappropriate content.*

#### *DBS School Website:*

- *Children are only referred to by their first names.*
- *No images of children will be labeled with names or shown close-up.*
- *Personal details like addresses or phone numbers are not shared on the website.*

### **STAFF PERSONAL SOCIAL MEDIA RESTRICTIONS**

- *Parental consent for filming students is strictly for the school's official use on approved social media and publications.*
- *Teachers are prohibited from sharing videos featuring students' faces on personal social media or with people outside the school.*
- *Such unauthorized sharing breaches confidentiality and undermines parental trust.*
- *Teachers may share innovative teaching practices or classroom setups if students' faces are not visible.*
- *All content involving students must follow the school's guidelines and be used only for official school representation.*

### **SAFETY POINTS FOR STUDENTS TO CONSIDER**

- *Use only your own login credentials to access school computers, the internet, and other tech equipment.*
- *Do not view, alter, or delete other people's work/files.*
- *Do not modify or delete any settings on school devices.*
- *Ask for permission before accessing any website unless already approved by a teacher.*
- *Only send emails that have been approved and reviewed by a teacher, ensuring the messages are polite and appropriate.*
- *Never share your personal information (name, address, phone number) or arrange meetings with anyone via email.*
- *Do not share others' personal information.*
- *Do not enter Internet chat rooms while using school computers.*
- *If you encounter something inappropriate or receive unpleasant messages, turn off the screen and immediately inform a teacher.*

### **CYBER BULLYING**

- *Cyberbullying involves bullying through communication technology like text messages, emails, or websites.*

- *Common forms include:*
- *Sending threatening or abusive text messages or emails, either personally or anonymously.*
- *Posting insulting comments about someone on websites or social networking sites.*
- *Sharing derogatory or embarrassing videos of someone via mobile phones or email.*
- *Cyberbullying, using any form of technology to bully others, will not be tolerated.*

### **INFORMATION FOR PARENTS:**

- *At DBS, cyberbullying is taken as seriously as other types of bullying and is addressed individually.*
- *Consequences may include:*
- *Verbal warnings.*
- *Parental discussions.*
- *More serious actions for severe cases.*
- *Cyberbullying can occur anonymously, 24/7 and is harder to detect as it leaves no physical scars.*
- *It can be highly intrusive and cause severe emotional harm, especially to young people.*
- *Young people often use acronyms in communication (e.g., POS, TUL), which can be difficult for adults to understand, increasing the challenge of identifying threats.*
- *Incidents can be reported to the division principals.*

### **POINTS FOR PARENTS TO CONSIDER AT HOME:**

*It is important to promote phone and Internet Safety in the home, and to monitor Internet use.*

*Tips to Promote Internet Safety at Home:*

- *Discuss the fact that there are websites which are unsuitable.*
- *Discuss how children should respond to unsuitable materials or requests.*
- *Remind children never to give out personal information on the Internet.*
- *Remind children that people online may not be who they say they are.*
- *Be vigilant. Ensure that children do not arrange to meet someone they meet online.*
- *Be aware that children may be using the Internet in places other than in their own home or at school.*
- *Be aware of the safety issues regarding mobile phones.*
- *Encourage children to talk about how they use mobile phones.*
- *Remind children not to give mobile numbers to strangers and people they do not know very well.*
- *Talk about responsible use of the internet and technology.*

### *Monitor Internet use:*

- *Keep the computer in a communal area of the home.*
- *Monitor online time and be aware of excessive hours spent on the Internet.*
- *Take an interest in what children are doing.*
- *Discuss with the children what they are seeing and using on the Internet.*
- *Advise children to take care and to use the Internet in a sensible and responsible manner.*
- *Check internet history log. This will tell you what websites your child is frequenting.*

### **FILTERING FOR THE HOME COMPUTER:**

- *Parents may wish to invest in security software for their children's computers.*
- *Some of this software works by monitoring all Internet activity for trigger words.*
- *There are many types of security software available, the following are only a few.*

*Examples include:*

- *Net Nanny*
- *Cyber Patrol*
- *Surfwatch*

### **INFORMATION FOR STUDENTS:**

#### **If you are being bullied:**

- *Remember, bullying is never your fault. It can be stopped, and it can usually be traced.*
- *Don't ignore the bullying. Tell someone you trust, such as a teacher or parent.*
- *Try to keep calm; if you are frightened, try to show it as little as possible.*
- *Don't get angry, it will only make the person bullying you more likely to continue.*

### **ON THE INTERNET:**

- *Don't share personal details online such as your address, school, or email, as it can help someone harm you.*
- *Save evidence of bullying, including emails, text messages, or images, to show to parents, teachers, or authorities.*

- Note the time, date, and details about the sender of any bullying messages or images.
- Seek online advice on how to handle cyberbullying, such as from resources like [www.kidscape.org](http://www.kidscape.org) and [www.wiredsafety.org](http://www.wiredsafety.org).

**HANDLING CYBER-SAFETY COMPLAINTS:**

- Prompt action is required if a complaint is made regarding cyberbullying or internet misuse.
- The facts of the case will need to be established, including whether the issue occurred outside of school or through home internet use.
- Transgressions by students will be handled according to the school’s behavior policy.
- In serious situations, the police must be contacted.
- Complaints about internet misuse will be dealt with by senior staff.
- Complaints about staff misuse should be referred to the division Principal.
- Complaints about a child protection nature will be handled according to the school’s child protection procedures.

**DOCUMENT CONTROL**

<b>COMPLIANCE</b>	
<b>Compliant with</b>	<i>Local legislation, CIS and NEASC</i>

<b>AUDIENCE</b>	
<b>Internal</b>	<i>All staff in Dasman Bilingual School</i>

<b>VERSION CONTROL</b>	
<b>Author</b>	<i>Samar Dizmen, Waseem Bacus &amp; Fay Khan</i>
<b>Implementation</b>	<i>Annually-August to June</i>
<b>Review date</b>	<i>1<sup>st</sup> June Annually</i>