Lüderitz Blue School
E-Safety Policy

1. SCHOOL STATEMENT

Lüderitz Blue School recognizes the significant role that technology and the internet play in education. Our objectives include:

i) Establishing comprehensive measures to ensure the online safety of learners, staff, volunteers, and all members of the school community.

ii) Implementing a proactive approach to online safety that empowers and educates our entire school community in the use of technology.

iii) Creating clear protocols for identifying, addressing, and escalating incidents when necessary.

2. POLICY GUIDANCE

i) This policy is informed by various guidelines from the UK Department for Education, including:

- Statutory Safeguarding Guidance
- The Keeping Children Safe in Education Acts
- Guidance on Protecting Children from Radicalisation
- Related advice on Preventing and Tackling Bullying, Searching, Screening, and Confiscation.

ii) This policy also aligns with the UK National Curriculum Programmes of Study for Computing.

iii) This document should be understood and followed alongside other school policies, including but not limited to:

- Lüderitz Blue School Safeguarding Policy
- Lüderitz Blue School Anti-Bullying Policy
- Lüderitz Blue School Acceptable Use of Technology Policy

3. ROLES AND RESPONSIBILITIES

i) The Heads of School are tasked with ensuring that staff comprehend this policy and that it is consistently applied throughout the school.

ii) The Designated Safeguarding Lead (DSL) oversees online safety and works with staff to manage any online safety issues or incidents, ensuring appropriate logging and resolution of incidents in line with this policy. The DSL is also responsible for training staff and liaising with external agencies when necessary, as well as providing reports on online safety if needed.

iii) The Computing Teacher is responsible for:

- Implementing filtering and monitoring systems that are regularly updated to protect learners from harmful online content and contact while at school, including extremist material.
- Securing and protecting the school's ICT systems from viruses and malware, with regular updates.
- Conducting weekly security checks and monitoring the ICT systems.
- Blocking access to dangerous websites and preventing the download of harmful files where possible.
- Logging and addressing online safety incidents as per this policy.
- Managing incidents of cyberbullying according to the school behaviour policy.

iv) All staff, including contractors, interns, and volunteers, are required to:

- Maintain an understanding of this policy.
- Implement the policy consistently.
- Adhere to acceptable use terms for the school's IT systems and internet, ensuring learners do the same.
- Collaborate with the DSL to log and address online safety incidents according to this policy.
- Address incidents of cyberbullying in line with the school behaviour policy.

v) Parents/guardians are encouraged to:

- Raise any concerns or questions regarding this policy with any staff member.
- Ensure their child understands and agrees to the acceptable use terms outlined in the School Welcome Pack.
- Familiarise themselves with the Advice for Parents/Guardians regarding Cyberbullying and E-Safety (APPENDIX A) if they have concerns.

vi) Visitors and community members using the school's IT systems or internet will be informed of this policy and are expected to comply with it. They may also be asked to agree to the acceptable use terms.

4. EDUCATING LEARNERS ABOUT ONLINE SAFETY

i) Learners will receive education on online safety during their Computing lessons.

ii) The safe use of social media and the internet may also be incorporated into other subjects, such as Citizenship.

iii) In Early Years and Key Stage 1, learners will learn to:

- Use technology safely and respectfully, safeguarding personal information.
- Identify sources of help and support for concerns about online content or contact.

iv) In Key Stage 2, learners will learn to:

- Use technology safely, respectfully, and responsibly.
- Recognize acceptable and unacceptable behaviour online.
- Identify ways to report concerns regarding online content and contact.

v) In Key Stage 3, learners will learn to:

- Use technology safely, respectfully, and securely, including protecting their online identity.
- Recognize inappropriate content, contact, and conduct, and know how to report concerns.

vi) In Key Stage 4 and 5, learners will learn to:

- Understand the impact of technology on safety, including new methods for protecting online privacy and identity.
- Report various concerns effectively.

vii) These topics may also be addressed during Assemblies or other school events.

5. NOTE ON EDUCATING PARENTS/GUARDIANS ABOUT ONLINE SAFETY

i) The school will enhance parents' and guardians' understanding of internet safety through communications and information shared on our school website.

ii) This policy is publicly accessible to parents and guardians via the school website.

iii) Queries or concerns regarding online safety should first be directed to the child's class teacher and/or the DSL.

iv) Any member of staff can be approached regarding concerns or questions about this policy.

6. EDUCATING LEARNERS ABOUT CYBERBULLYING

i) Cyberbullying is recognized as a form of bullying occurring online, such as through social networking sites, messaging apps, or gaming platforms.

ii) Similar to other bullying forms, it involves repetitive and intentional harm inflicted by one individual or group onto another. It is characterised by a power imbalance.

iii) The school aims to prevent and address cyberbullying by:

- Ensuring learners understand what it is and how to respond if they witness it or experience it themselves.
- Informing learners about the reporting processes for any incidents.
- Engaging in discussions about cyberbullying, clarifying its reasons, potential forms, and consequences.
- Addressing the topic in class discussions and assemblies.
- Integrating cyberbullying education into relevant academic lessons (e.g., Citizenship and Computing).
- Providing resources on cyberbullying for parents to help them recognize signs, reporting processes, and ways to support affected children (see APPENDIX A).

iv) In response to specific cyberbullying incidents, the school will follow the procedures outlined in the Behavior Policy. If harmful or illegal content has been disseminated, the school will take reasonable measures to contain the incident.

v) The DSL will evaluate whether any incident involving illegal content should be reported to the police and will collaborate with external services as needed.

vi) Staff may search for and, if necessary, delete inappropriate files or images on learners' devices, including mobile phones and tablets, when there is a "good reason" to do so.

vii) Learners must grant full access to all areas of their personal devices, including password-protected sections, when requested.

viii) When determining whether there is a valid reason to examine or erase data, staff must reasonably suspect that the data in question has been or could be used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Violate school rules.

ix) If inappropriate material is found on a device, the DSL or another member of the senior leadership team will decide whether to delete it, retain it as evidence, or report it to the police.

x) Any searches of learners will comply with current international guidance on screening, searching, and confiscation, as well as Namibian law.

xi) Complaints regarding searches or the deletion of inappropriate content on learners' devices will be handled through the school's complaints procedure.

7. ACCEPTABLE USE OF TECHNOLOGY

i) All learners, parents, staff, volunteers, and governors must sign an agreement outlining acceptable use of the school's IT systems and internet.

ii) Visitors must read and agree to the school's acceptable use terms if applicable.

iii) Use of the school's internet is restricted to educational purposes or tasks related to fulfilling one's role.

iv) Lüderitz Blue School will monitor website access by learners, staff, volunteers, interns, and visitors (when applicable) to ensure compliance.

v) For additional information, refer to the Lüderitz Blue School Acceptable Use of Technology Policy.

8. NOTE ON STAFF USING WORK DEVICES OUTSIDE OF SCHOOL

i) Staff using work devices off school premises must not install unauthorised software or violate the school's acceptable use policy.

ii) Staff must secure their work devices with passwords and avoid sharing these passwords. USB devices containing school data must be encrypted.

iii) Staff should consult the Computing Teacher or Head of School if they have security concerns.

iv) Work devices are to be used solely for professional purposes.

v) For further details, refer to the Lüderitz Blue School Acceptable Use of Technology Policy.

9. RESPONSE TO MISUSE

i) When a learner misuses the school's IT systems or internet, the procedures outlined in the Behavior Policy will be followed. The response will vary based on the individual circumstances, nature, and severity of the incident.

ii) If a staff member misuses the school's IT systems or internet, or misuses a personal device in a manner that constitutes misconduct, the issue will be addressed according to staff disciplinary procedures.

iii) The response will depend on the specific circumstances, nature, and seriousness of the incident.

iv) Lüderitz Blue School will assess whether incidents involving illegal activity or serious misconduct should be reported to the police.

10. NOTE ON TRAINING

i) All new staff receive Safeguarding Training during their induction at Lüderitz Blue School.

ii) This training encompasses E-Safety and Cyberbullying topics.

iii) More specialised training will be provided when possible.

iv) Additional training updates will be included in Safeguarding sessions, along with other relevant communications (e.g., through Professional learning sessions, emails, and staff meetings).

v) Volunteers will also receive appropriate training and updates as needed.

vi) Staff are encouraged to review the Online Safety Training Needs – Self-audit for Staff (APPENDIX B) to assess their training requirements.

vii) Should further training be needed, staff are encouraged to contact the Head of School to arrange it.

11. NOTE ON SOCIAL MEDIA AND PHOTOGRAPHY/RECORDING

i) Lüderitz Blue School encourages the responsible use of social media by staff, learners, and parents to promote school activities and achievements.

ii) Staff are advised to maintain professional boundaries online, avoiding personal relationships with learners or their families through social media platforms.

iii) When posting images or videos of learners on social media, staff must ensure that parental consent has been obtained in accordance with the school's policies on photography and data protection.

iv) Learners and parents must understand the importance of seeking permission before sharing images or videos of others, especially in educational settings.

v) The use of personal devices to capture photos or videos of school events is permitted, provided that it aligns with the school's policies and consent has been secured.

vi) Staff should avoid sharing sensitive information about learners or the school on social media.

vii) Any concerns regarding the misuse of social media or photography should be reported to the DSL.

12. MONITORING AND REVIEW OF THIS POLICY

i) This E-Safety Policy will be reviewed annually or in response to specific incidents or developments in technology.

ii) Feedback from learners, staff, and parents will be considered during the review process to ensure that the policy remains effective and relevant.

iii) The DSL will be responsible for overseeing the policy review and ensuring that all stakeholders are informed of any changes.

iv) The updated policy will be shared with all staff, parents, and the school community via the school's website and during appropriate school meetings.

Written/Reviewed: Senior Management, 2024
Next Review Due: May 2025

APPENDIX A

Advice for Parents/Guardians regarding Cyberbullying and E-Safety

USEFUL WEBSITES

Parents/guardians can seek further guidance on keeping children safe online (including from Cyberbullying) from the following organisations and websites:

Hot topics, Childnet International:
http://www.childnet.com/parents-and-carers/hot-topics
InternetMatters
https://www.internetmatters.org/
Parent factsheet, Childnet International:
http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
KidsHealth: Cyberbullying
https://kidshealth.org/en/parents/cyberbullying.html

HELPFUL TIPS

- **Educate Your Child**: Explain what cyberbullying is, how it can affect individuals, and why it's essential to treat others with respect online.
- **Encourage Open Communication**: Foster an environment where your child feels comfortable discussing their online experiences with you, including any negative interactions they may face.
- **Establish Clear Rules**: Set specific guidelines regarding internet and social media usage, including time limits and acceptable online behaviour.
- **Monitor Online Activity**: Keep an eye on your child's online interactions to ensure their safety while respecting their privacy. Consider using parental controls when appropriate.
- **Promote Kindness and Empathy**: Encourage your child to engage in positive interactions and to be supportive of their peers, highlighting the importance of kindness in all communications.
- **Familiarise Yourself with Platforms**: Take the time to learn about the apps and websites your child uses. Understanding these platforms can help you identify potential risks.
- **Utilise Privacy Settings**: Help your child set their social media profiles and accounts to private, limiting who can view their information and posts.
- **Teach Reporting and Blocking**: Ensure your child knows how to report and block abusive users or content across different platforms.
- **Be a Positive Role Model**: Demonstrate responsible and respectful online behaviour. Your actions can significantly influence your child's attitude toward their own online conduct.
- **Stay Informed**: Keep yourself updated on the latest trends, apps, and potential risks associated with online behaviour to better guide your child.
- **Encourage Critical Thinking**: Teach your child to think critically about the content they encounter online, including understanding the difference between real and false information.
- **Discuss the Importance of Digital Footprint**: Help your child understand that their online actions can have long-term consequences and the importance of maintaining a positive digital presence.

APPENDIX B

Online Safety Training Needs – Self-Audit for Staff

1. Are you aware of who holds the lead responsibility for online safety within the school?

2. Do you know the appropriate steps to take if a learner approaches you with a concern or issue?

3. Are you familiar with the school's Acceptable Use Statement for staff, volunteers, governors, and visitors?

4. Are you familiar with the school's Acceptable Use Statement for learners?

5. Do you regularly update your password for accessing the school's IT systems?

6. Are you knowledgeable about the school's policy regarding cyberbullying?

7. Are there specific areas of online safety where you would like to receive training or further training?