Lüderitz Blue School
E-Safety Policy

1. STATEMENT ON E-SAFETY

Lüderitz Blue School understands the importance of the internet and technology and the role it plays in education. As a school, we aim to:

i) have robust processes in place to ensure the online safety of learners, staff, volunteers and other members of the school community.

ii) deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.

iii) establish clear procedures to identify, intervene and escalate an incident, where appropriate.

2. POLICY GUIDANCE

i) This policy is based on various guidance documents from the UK Department for Education, such as

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

ii) This policy also takes into account the UK National Curriculum Programmes of Study for Computing.

iii) This policy should be read, understood and followed alongside other policies of the school, 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 responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

ii) The DSL (Designated Safeguarding Lead) takes lead responsibility for online safety in school including

- working together with all staff to address any online safety issues or incidents.
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy.
- updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing reports on online safety in school, if required.

iii) The Computing Teacher is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep learners safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

iv) All staff, including contractors, interns and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet and ensuring that learners follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

v) Parents are expected to:

- Notify any member of staff with any concerns or queries regarding this policy.

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (provided in the School Welcome Pack).
- In case of concern, to familiarise themselves with the provided Advice for Parents/Guardians regarding Cyberbullying and E-Safety (APPENDIX A).

vi) Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. EDUCATING LEARNERS ABOUT ONLINE SAFETY

i) Learners are taught about online safety in their Computing lessons.

ii) Where appropriate, the safe use of social media and the internet will also be referred to in other subjects, such as Citizenship.

iii) In Early Years and Key Stage 1, learners are taught to:
- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

iv) In Key Stage 2, learners are taught to:
- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

v) In Key Stage 3, learners are taught to:
- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

vi) In Key Stage 4 and 5, learners are taught:
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

vii) These topics may also be covered in Assembly or other school events.

5. NOTE ON EDUCATING PARENTS/GUARDIANS ABOUT ONLINE SAFETY

i) The school will raise parents' and guardians' awareness of internet safety in communications or other communications home, and in information via our school website.

ii) This policy is also publically available to parents/guardians on our school website.

iii) If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the child's class teacher and/or the DSL.

iv) Concerns or queries about this policy can be raised with any member of staff.

6. EDUCATING LEARNERS ABOUT CYBERBULLYING

i) Cyberbullying can be defined as a form of bullying which takes place online, such as through social networking sites, messaging apps or gaming sites.

ii) Just as other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

iii) The school aims to address and prevent cyber-bullying by:

- ensuring that learners understand what it is and what to do if they become aware of it happening to them or others.
- ensuring that learners know how they can report any incidents.
- actively discussing cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- discussing cyber-bullying within classes, and addressing the issue in assemblies.
- covering cyber-bullying in academic lessons as is appropriate (eg. in Citizenship and Computing).
- making information on cyber-bullying available to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. Please see APPENDIX A - Tips for parents/guardians about addressing and preventing cyberbullying.

iv) In the case of a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among learners, the school will use all reasonable endeavours to ensure the incident is contained.

v) The DSL will consider whether an incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

vi) School staff may search for and, if necessary, delete inappropriate images or files on learners' electronic devices, including mobile phones, iPads and other tablet devices, where the Head of Section believes there is a 'good reason' to do so.

vii) Learners are required to allow full access to all areas of a personal device, including password-protected areas, in such cases.

viii) When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

ix) If inappropriate material is found on the device, it is up to the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

x) Any searching of learners will be carried out in line with the latest international guidance on screening, searching and confiscation, and with Namibian law.

xi) Any complaints about searching for or deleting inappropriate images or files on learners' electronic devices will be dealt with through the school complaints procedure.

7. ACCEPTABLE USE OF TECHNOLOGY

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

ii) Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

iii) Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

iv) Lüderitz Blue School monitors the websites visited by learners, staff, volunteers, interns and visitors (where relevant) to ensure they comply with the above.

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

8. NOTE ON STAFF USING WORK DEVICES OUTSIDE OF SCHOOL

i) Staff using a work device outside school must not install unauthorised software or violate the school's acceptable use policy.

ii) Staff must keep their work device secure and password-protected, and not share their password. USB devices with school data must be encrypted.

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

iv) Work devices must be used only for work purposes.

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

9. RESPONSE TO MISUSE

i) If a learner misuses the school's IT systems or internet, the school follows the procedures set out in the Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

ii) If a staff member misuses the school's IT systems or the internet, or misuses a personal device and the action constitutes misconduct, the matter will be dealt with in accordance with staff disciplinary procedures.

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

iv) Lüderitz Blue School will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. NOTE ON TRAINING

i) All new staff members receive Safeguarding Training, as part of their induction at Lüderitz Blue School.

ii) This training covers ESafety and Cyberbullying.

iii) Where possible, more specific training will be provided.

iv) Additional training will be provided as part of Safeguarding training, as well as relevant updates as required (for example through Professional learning sessions, emails and staff meetings).

v) Where applicable, volunteers will receive appropriate training and updates.

vi) Staff are encouraged to refer to the Online Safety Training Needs – Self-audit for Staff (APPENDIX B) to reflect on whether more training is required.

vii) If more training is required, staff are encouraged to contact the Head of School to arrange this.

11. NOTE ON SOCIAL MEDIA AND PHOTOGRAPHY/RECORDING

For Child Protection and Safeguarding reasons, the following rules apply to parents and staff:

i) Do not take photos or make recordings on school premises or during events without the permission of your Head of Section.

ii) Do not share or upload images taken on school campus or during events to personal social media channels. An exception is when staff repost from the official school social media channels.

iii) Staff must not connect with learners on social media, or former learners until at least two years after they leave the school or reach school-leaving age, whichever is later.

iv) Staff who are also parents may share images but must remain aware of their professional responsibilities.

v) Staff must not comment on the school in personal social media with any negative comments or connotations.

vi) Staff must maintain appropriate privacy levels in all social media activities to protect the school's reputation.

11. NOTE ON MONITORING

i) The DSL keeps a log of behaviour and safeguarding issues related to online safety.

ii) This policy will be reviewed annually by the Head of School and shared with the Chair of the School Board.

Written: 08.05.24
Written by: Christian Bishop
Reviewed by: Marnie Allen
Next review due: May 2025

APPENDIX A

Advice for Parents/Guardians regarding Cyberbullying and E-Safety

ESAFETY
Parents/guardians can seek further guidance on keeping children safe online from the following organisations and websites: *Hot topics, Childnet International:* http://www.childnet.com/parents-and-carers/hot-topics *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
CYBERBULLYING
Parents/guardians can follow these tips for guidance regarding prevention of cyberbullying: • Educate Your Child: Teach them about what cyberbullying is and its impact. • Open Communication: Encourage your child to talk to you about their online experiences. • Set Rules: Establish clear guidelines for internet and social media use. • Monitor Activity: Keep an eye on your child's online interactions, but respect their privacy. • Promote Kindness: Encourage respectful and kind behaviour online. • Know the Platforms: Familiarise yourself with the apps and websites your child uses • Use Privacy Settings: Ensure your child's profiles are set to private. • Report and Block: Teach your child how to report and block abusive users. • Be a Role Model: Demonstrate positive online behaviour yourself. • Stay Informed: Keep up-to-date with the latest trends and risks in online behaviour.

APPENDIX B

Online Safety Training Needs – Self-audit for Staff

- Do you know the name of the person who has lead responsibility for online safety in school?
- Do you know what you must do if a learner approaches you with a concern or issue?
- Are you familiar with the school's Acceptable Use Statement for staff, volunteers, governors and visitors?
- Are you familiar with the school's Acceptable Use Statement for learners?
- Do you regularly change your password for accessing the school's IT systems?
- Are you familiar with the school policy on cyber-bullying?
- Are there any areas of online safety in which you would like training/further training? Please record them here.