Purple Ruler Online Safety Policy

Document Authors Name	Bella Ma Daniel Demarmels
Approved By	Daniel Demarmels

Document Version Control	
Creation Date	July 2024
Review and Revision Date	July 2025

Introduction

In the digital age, online safety is paramount to safeguarding the well-being of learners and staff. With the increasing reliance on digital tools and online learning platforms, it is essential to establish a comprehensive Online Safety Policy that aligns with legal and regulatory standards. This policy aims to protect all users from online risks, promote responsible use of digital technologies, and ensure a secure and supportive learning environment.

Our organization recognizes the importance of educating learners and staff about the potential dangers and benefits of online interactions. This policy outlines the roles and responsibilities of

all stakeholders, including learners, staff, parents, and administrators, in fostering a culture of online safety. By implementing this policy, we commit to providing ongoing training, clear reporting procedures, and robust safeguards to address online safety issues promptly and effectively.

This policy complies with key legislative and regulatory frameworks, including the “Keeping Children Safe in Education” (KCSIE) guidelines, the Online Education Provider Accreditation Scheme, and other relevant laws and standards. It serves as a foundation for our efforts to create a safe digital environment that supports the educational and personal development of all users.

Policy Aims

The aims of our Online Safety Policy are multifaceted, reflecting the complex and evolving nature of digital technology in education. Our policy aims to:

Safeguard All Users: Protecting learners and staff from the myriad risks associated with online activities is our foremost priority. This includes shielding them from cyberbullying, exposure to inappropriate content, online predators, and any form of digital exploitation. We strive to create a secure online environment where everyone feels safe and supported.

Promote Responsible Use: Encourage and educate all users on the responsible and ethical use of digital technologies. This includes understanding digital etiquette, respecting privacy, and recognizing the implications of one’s digital footprint. By fostering responsible use, we aim to cultivate a respectful and positive online community.

Ensure Legal and Regulatory Compliance: Adhere strictly to all relevant legislation and guidelines, including the “Keeping Children Safe in Education” (KCSIE) guidelines, General Data Protection Regulation (GDPR), Children Act 1989 and 2004, The Prevent Duty, Education Act 2002, and Equality Act 2010. Compliance ensures that our policies and practices are up-to-date and legally sound, providing a safe learning environment for all.

Provide Clear Framework for Reporting and Management: Establish straightforward and accessible procedures for reporting online safety incidents. This includes clear guidelines on how incidents are managed, investigated, and resolved, ensuring timely and effective responses to any issues that arise.

Support and Educate the School Community: Offer continuous education and support to learners, staff, and parents on online safety issues. This involves regular training sessions,

workshops, and access to resources that help the school community stay informed about the latest online safety practices and threats.

Facilitate Safe Digital Learning: Ensure that our digital learning platforms and tools are used safely and effectively to enhance education. This includes setting up proper security measures, monitoring online activities, and providing guidelines on the safe use of technology in educational contexts.

Empower Learners with Digital Literacy: Equip learners with the knowledge and skills necessary to navigate the digital world safely and confidently. This includes teaching them how to recognize and avoid online risks, how to seek help when needed, and how to use digital tools responsibly and effectively.

Create a Culture of Online Safety: Foster an organizational culture that prioritizes online safety, where all members of the school community understand their roles and responsibilities in maintaining a safe online environment. This cultural shift is crucial in ensuring that online safety becomes an integral part of our educational framework.

Scope

This Online Safety Policy applies to all members of our educational community, including learners, staff, parents, and volunteers. It is designed to provide a safe and secure online environment, whether individuals are using personal or institutional devices, and regardless of the physical location from which they access digital resources.

Learners

Learners are expected to engage with online resources and digital tools in a manner that is safe, respectful, and conducive to learning. They should be aware of the potential risks associated with online activities and adhere to the guidelines and instructions provided to ensure their online behaviour aligns with the school’ s safety standards.

Staff

Staff members are responsible for modelling appropriate online behaviour and for ensuring that the educational content delivered through digital platforms is secure and appropriate. They must adhere to the guidelines set forth in this policy and take an active role in educating learners about online safety practices.

Parents and Guardians

Parents and guardians play a crucial role in supporting the online safety measures implemented by the school. They are encouraged to reinforce the principles of safe online behaviour at home and to monitor their children’ s internet use to ensure it aligns with the safety protocols outlined in this policy.

Volunteers

Volunteers who interact with learners or have access to the school’ s digital resources must adhere to the same standards of online conduct as staff members. They are expected to support the school’ s online safety efforts and report any concerns or incidents in accordance with the procedures outlined in this policy.

Third-Party Providers

Any third-party service providers or contractors who have access to the school’ s digital platforms or data are required to comply with this Online Safety Policy. They must ensure that their services do not compromise the safety and security of the school’ s online environment and adhere to all relevant data protection regulations.

Application Across All Digital Platforms

This policy applies to all digital and online platforms used within the school’ s educational framework. This includes, but is not limited to, learning management systems, email, social media, video conferencing tools, and any other digital communication tools. It is designed to be flexible to address the evolving nature of technology and the internet, ensuring that all users are protected regardless of the tools or platforms they use.

Legislative and Regulatory Compliance

This Online Safety Policy aligns with key legislative and regulatory requirements, including Keeping Children Safe in Education (KCSIE), the General Data Protection Regulation (GDPR), and other relevant UK legislation. It is designed to ensure compliance with these standards, thereby safeguarding the rights and safety of all members of the school community in their online interactions.

Roles and Responsibilities

Director Team

The SLT holds ultimate responsibility for ensuring the implementation of this Online Safety Policy and integrating it within the school’ s overall safeguarding framework. Their roles include:

- Leading the development and regular review of the Online Safety Policy, ensuring it aligns with national standards and statutory requirements such as Keeping Children Safe in Education (KCSIE).
- Ensuring that adequate resources are allocated for effective implementation of the policy, including training, technology, and support systems.
- Overseeing the monitoring and evaluation processes to assess the effectiveness of online safety measures and making adjustments as necessary.
- Appointing a third party service to support the implementation and maintenance of technical security measures such as firewalls, antivirus software, and internet filtering systems to protect against online threats.
- Regularly monitoring and auditing the organisation's cloud systems and database to detect and respond to any breaches or potential risks.
- Providing technical support and guidance to staff and learners to ensure safe and effective use of the organisation's cloud based resources.

Designated Safeguarding Lead (DSL)

The DSL is the primary point of contact for all online safety concerns and is responsible for:

- Managing and responding to online safety incidents in accordance with the school’ s safeguarding and child protection policies.
- Leading the development and delivery of online safety training for staff and learners, ensuring they are aware of risks and know how to respond to online safety issues.
- Ensuring that the Online Safety Policy is implemented effectively across the school and that staff understand their roles in maintaining a safe online environment.

Management Team

The management team have a duty of care towards teaching staff and learners, ensuring that the online safety policy is implemented well in practice. They are also responsible for supporting the DSL.

- To provide training, instructional information and support for facilitators and learners in using the learning systems appropriately, safely and effectively.
- To monitor facilitator and learner's appropriate use of online learning platform.

- Report incidents of any concerns in a timely manner.
- To assist facilitators and direct them to the correct method of reporting incidents where necessary.
- To support the DSL where necessary in managing an incident.
- To monitor and review the implementation of the online safety policy, to make recommendations to the DSL and Director team on ways of improving the policy and practice.

Teaching Staff

All teaching and support staff have a duty to promote and ensure online safety within their educational practices. Their responsibilities include:

- Demonstrating positive online behaviours and adhering to the Online Safety Policy in all professional activities.
- Integrating online safety education within the curriculum and addressing online safety issues as part of teaching and learning activities.
- Reporting any online safety concerns or incidents to the DSL in a timely and appropriate manner.

Learners

Learners are expected to take an active role in their own online safety and the safety of their peers. Their responsibilities include:

- Following the guidelines and rules set out in the school’ s Online Safety Policy and Acceptable Use Agreements.
- Reporting any online safety issues or concerns to a trusted adult, such as a facilitator or the DSL.
- Engaging in safe and responsible online behaviour, including protecting personal information and respecting others online.

Parents and Guardians

Parents and guardians play a crucial role in supporting the online safety measures implemented by the school. Their responsibilities include:

- Creating a safe online environment at home by setting appropriate boundaries and monitoring their children’ s internet use.

- Collaborating with the organisation to reinforce online safety messages and attending any training or information sessions offered by the organisation.
- Communicating with the organisation if they have any concerns about their child’ s online safety or if they become aware of any incidents.

Acceptable Use Agreements

With whom to sign:

- All learners who are age 13 and above, who will be using the organisation’ s digital platforms should sign the AUA.
- Parents or guardians should sign the AUA alongside their children, especially for learners who are below the age of 13, to acknowledge their role in supervising and supporting their children’ s online activities.
- All teaching and non-teaching staff who will be using or overseeing the use of digital platforms need to sign the AUA.
- Any volunteers who will have access to the organisation’ s digital resources or interact with learners online should sign the AUA.
- Any external personnel, such as guest speakers or temporary workers, who will use the organisation’ s digital systems, should sign the AUA before they are granted access.

When to Sign:

- **New Learners**: Upon enrolment and before they begin using any of the organisation’ s digital platforms.
- **Returning Learners**: At the start of each academic year to reinforce the importance of safe and responsible use of digital technologies.
- **New Staff Members**: During the induction process and before accessing any digital platforms or tools provided by the organisation.
- **Current Staff Members**: Annually, typically after the online safety policy is reviewed and updated, to ensure continued compliance with the updated policies.
- **Volunteers and Visitors**: Before they access any digital platforms or engage in activities involving the organisation’ s digital environment.
- **Parents/Guardians**: When their children are first enrolled, to ensure they understand and agree to the terms of responsible digital use that their children must follow. Then again, possibly annually after the online safety policy is reviewed with updated information.

Online Safety Education and Training

Staff Training and Professional Development

Ensuring that all staff are well-equipped to handle online safety issues is essential. This section outlines the continuous training and professional development provided to staff:

Initial Training:

- New staff members receive comprehensive training on online safety policies, including the Acceptable Use Agreement and procedures for reporting incidents.
- Introduction to the organisation’ s online safety protocols, an overview of the legal framework, and practical guidance on safeguarding children in an online environment.

Ongoing Professional Development:

- Articles and relevant information will be sent to update staff on the latest trends in online safety, emerging threats, and new legislative requirements.
- Workshops will be held to update staff on updated protocols during term time.
- Mandatory annual courses to ensure staff remain up-to-date with best practices and any changes in policies.
- Targeted training for roles with specific online safety responsibilities, such as the DSL.
- A dedicated online portal providing access to the latest research, resources, and best practices in online safety.

Evaluation and Feedback:

Regular assessments and feedback surveys to gauge the effectiveness of training programs and identify areas for improvement.

Learner Online Safety Curriculum

Online safety is built into our Digital Functional Skills curriculum to ensure learners are aware of the potential risks they are exposed to online, however, ensuring they learn the necessary skills to identify those risks and preventative strategies from harm.

Purple Ruler Digital Functional Skills Scheme of Work

Parental Engagement and Education

Engaging parents and guardians in online safety is essential to ensure that learners are supported both at school and at home, we will use the following methods to achieve this:

- Offering workshops and seminars to educate parents on the risks their children may face online and how they can help mitigate these risks.
- Send out newsletters providing tips, updates on the latest online safety trends.
- A dedicated section on the learner/parent portal where parents can access resources, guides, and tools to support their child’ s online safety.

Safe Use of Digital Platforms

Ensuring the safe use of digital platforms is a critical component of our online safety policy. As our organisation does not provide IT equipment for learners or staff, we must emphasise best practices and guidelines that safeguard the online activities of all users, regardless of the device or network they use. This section outlines the principles and measures that must be adhered to for maintaining a safe digital environment.

Approved Platforms

- Only approved platforms are to be used for conducting online classes, group work, and communication between Learners, staff, and parents.
- The primary digital platform used for management, operation, communication and for Learner learning for full time Learners is Lark.
- The COO is responsible for the regular review and approval of digital platforms to ensure they meet our security and safeguarding standards.
- Facilitators must share their screen if they need to use resources from websites rather than sending links of the website directly to the learners to use, unless it is an approved platform.

Account Creation and Management:

- There are different permission levels set for accounts used by different roles. For example, the directors and some senior managers have Admin level permission on Lark, which will allow them to customise settings of the system as required. Mid-Level managers have manager level permission, which allows them to access certain data but not able to change any systematic settings.
- Admin accounts are provided by the COO. Learner accounts can be set up by managers.
- Learner accounts on Lark only has permission to access the documents, groups, contacts, calendar and video recordings that are associated with their course that's specifically set up for them by the organisation.

- Facilitators and Learners do not have the ability to contact anyone within the organisation directly by the search box, other than the management team. Facilitators and Learners will have a group chat set up for them by the admin team at the beginning of their courses and disbanded when the learner no longer learns with this particular facilitator.
- Facilitators and learners will have their own individual peer groups, which is monitored by the management team. This provides a safe space for each peer group to share ideas, socialise and build a community.
- We recognise that there is a chance that each peer group may exchange personal contact details, whilst this isn't prohibited however, all communication related to Purple Ruler activities must take place on Lark or another approved platform. This is to ensure we can monitor and mediate any situations.
- Learners who socialises outside of our digital workplace and encounters bullying or other forms of abuse will be approached by following the anti-bullying and safeguarding policies.

Parental Access:

Parents will be encouraged to create an individual external account outside of the organisation and added as an external contact. They are not able to access recordings of the sessions unless the lesson is a one to one only with their child. They can only communicate in the group chat that has been set up for them.

Lessonspace:

- Only Purple Ruler staff have accounts to Lessonspace. Admin and managers has access to all lesson recordings. Facilitators has access to lesson recordings of their own lessons.
- Schools will be granted permission to view specific recordings of their own Learners upon request of a valid reason, such as Facilitator performance, safeguarding or behavioural issues.
- The COO monitors the activities and use of Lessonspace on a weekly basis.

Social Media and Public Platforms

- Staff should maintain professional boundaries when using social media. They should avoid connecting with learners on personal social media accounts. More details on this in the Staff Code of Conduct.
- We advise against sharing personal information or sensitive content on public platforms. Use Purple Ruler -approved channels for official communications and announcements.

- Any incidences of anti-bullying or other forms of abuse, harm identified on social media or public platforms should be reported by using the anti-bullying and safeguarding policies.

Cybersecurity Measures

1. **Incident Detection and Reporting**

- **Monitoring Systems:** Our organization utilizes advanced monitoring software, such as Guard Dog, to detect unusual activities or breaches in our digital environment, such as out-of-date software which can lead to vulnerabilities in our cybersecurity infrastructure. All systems are regularly reviewed to ensure they are functioning correctly and updated to respond to new threats.
- **Reporting Mechanisms:** Clear procedures are in place for reporting cybersecurity incidents. A designated email address or reporting tool is accessible to learners, staff, and parents for this purpose. This is DSO@purpleruler.com

2. **Immediate Response Procedures**

- **Initial Assessment:** Upon detection of a potential cybersecurity incident, an initial assessment is conducted to determine the severity and nature of the issue. This includes identifying whether the incident involves personal data, cyberbullying, inappropriate content, or other online safety issues.
- **Containment:** Immediate steps are taken to contain the incident. This may involve isolating affected systems, disabling compromised accounts, or blocking harmful content to prevent further damage.
- **Communication:** Relevant parties, including the DSLs, IT staff, and leadership team, are promptly notified about the incident and the actions being taken.

3. **Investigation**

- **Gathering Evidence:** A thorough investigation is conducted to gather all relevant data, logs, and evidence related to the incident. This is done while maintaining a strict chain of custody to ensure the integrity of the evidence.
- **Interviews:** Interviews with individuals involved or witnesses are conducted to gather more detailed information about the incident.
- **Documentation:** Detailed records of the incident, including the nature of the issue, actions taken, and communications made, are maintained for future reference and analysis.

4. **Resolution and Recovery**

- **Remediation:** After containing the incident, steps are implemented to address the root cause and prevent recurrence. This may include updating software, changing passwords, or enhancing security measures.
- **Support for Affected Parties:** We provide support and counseling for individuals affected by the incident, such as victims of cyberbullying or those whose data was compromised.
- **Communication:** Once the incident is resolved, all relevant stakeholders are informed of the resolution and any measures taken to prevent future occurrences.

5. **Review and Improvement**

- **Post-Incident Review:** After an incident, a thorough review is conducted to understand what happened, how it was handled, and what improvements can be made. This process helps to enhance our overall cybersecurity posture.
- **Policy and Procedure Updates:** Based on the findings from the post-incident review, policies and procedures are updated to strengthen our cybersecurity measures and better protect against future incidents.
- **Training and Education:** Additional training is provided to staff and learners to address any gaps identified during the incident, ensuring that everyone is better equipped to handle similar issues in the future.

6. **Data Storage and Backup**

- **Secure Data Storage:** All sensitive data must be stored securely using encryption and other best practices. Staff members are required to save documents, presentations, and data relating to their work on Lark, as directed by their line managers. Sensitive data cannot be downloaded or copied and pasted.
- **Backup Protocols:** Our organization has implemented a backup regime that enables the recovery of critical systems and data within a reasonable timeframe in the event of a data loss. This includes the use of a remote location for encrypted backups.
- **Testing Backup Systems:** Regular testing of backup methods is conducted to ensure their reliability. This includes renaming and retrieving sample files from the backup to verify the system's effectiveness.

7. **Password Security**

- **Strong Passwords:** All staff and students are required to use strong passwords that contain at least eight characters, including upper and lower case letters, numbers, and special characters. Passwords should be changed every three months.
- **Password Confidentiality:** Passwords must not be written down or shared with others. Staff are also requito enable two-factor authentication (2FA) for an additional layer of security.

Incident Management

Incident Management Policy

Our organization is committed to a proactive and responsive approach to managing incidents that may compromise the safety, security, or integrity of our digital environment. This policy outlines the procedures for detecting, reporting, responding to, and reviewing incidents related to online safety and cybersecurity.

1. **Incident Detection and Reporting**

- **Monitoring Systems:**
  - We utilize Guard Dog monitoring tools to detect potential security breaches and unusual activities. Regular updates ensure these tools remain effective against emerging threats.
- **Reporting Mechanisms:**
  - Clear and accessible reporting channels are available for staff, learners, and parents. Incidents can be reported via a designated email or an online reporting tool, with options for anonymous reporting to encourage prompt communication. The email DPO@purpleruler.com is monitored by the Data Protection Officer who will respond to requests.

2. **Immediate Response Procedures**

- **Initial Assessment:**
  - Upon receiving an incident report, the designated team, led by the DPO, will assess the severity and nature of the incident to determine the appropriate response.
- **Containment:**
  - Immediate action will be taken to contain the incident, such as isolating affected systems, disabling compromised Lark or Wix accounts, or blocking harmful content to prevent further damage.
- **Notification:**
  - Relevant internal stakeholders, including the DPO and leadership team, will be promptly informed. Depending on the incident's severity, external authorities or affected individuals may also be notified.

3. **Investigation**

- **Evidence Collection:**
  - The incident response team will gather relevant data, logs, and other evidence while ensuring that the chain of custody is maintained for legal and internal review purposes.
- **Analysis and Interviews:**
  - A thorough analysis of the incident will be conducted, including interviews with involved parties to understand the incident's context and scope.
- **Documentation:**
  - All findings, actions taken, and communications will be meticulously documented to ensure a comprehensive incident record.

4. **Resolution and Recovery**

- **Remediation:**
  - Steps will be taken to resolve the incident, address the root cause, and restore normal operations. This may include software updates, security enhancements, or changes to procedures.
- **Support for Affected Parties:**
  - Those impacted by the incident, such as victims of cyberbullying or data breaches, will receive appropriate support and guidance throughout the resolution process.
- **Communication:**
  - Once resolved, all relevant stakeholders will be informed about the incident's resolution, the measures taken, and any steps to prevent future occurrences.

5. **Review and Improvement**

- **Post-Incident Review:**
  - After the incident is resolved, a review will be conducted to evaluate the response's effectiveness and identify areas for improvement.
- **Policy Updates:**
  - Based on the review's findings, policies and procedures will be updated to enhance our incident management capabilities.
- **Training and Awareness:**
  - Additional training and awareness initiatives will be implemented to address any gaps identified and improve future incident responses.

Monitoring and Review

1. **Regular Audits**:

- Conduct regular audits of our e-safety practices and policies.
- Use audit findings to improve and update the e-safety policy.

2. **Policy Review**:
   - Review the e-safety policy annually to ensure it remains relevant and effective.
   - Involve learners, staff, and parents in the review process to gather comprehensive feedback.

Resources and Support

Appendices

· **Sample Acceptable Use Agreements**: Templates for learners, staff, and parents/guardians.

· **Relevant Contact Information**: Key contacts for reporting and support.

· **Incident Reporting Forms**: Templates for reporting online safety incidents.

· **Reference Documents and Further Reading**: Additional resources and guidelines for further information.