CROWN PRIVATE SCHOOL مدرسة كراون الخاصة British Curriculum المنهاج البريطاني		ONLINE SAFETY POLICY

PROCESS NAME:	Online Safety Policy	**CREATION DATE:**	10/09/2022
PROCESS MANAGER:	IT Administrator	**LAST REVISION:**	05/02/2025
APPLIES TO:	All Staff All Parents All Children	**RELATED DOCUMENT(S):**	Acceptable Use Policy

1. Introduction

This **Online Safety Policy** outlines the procedures and responsibilities in place at Crown Private School to protect all members of the school community from online risks. The policy aims to safeguard students, staff, and other stakeholders from cyberbullying, data breaches, exposure to inappropriate content, and other online safety threats. It also promotes responsible online behavior and digital literacy.

2. Scope

This policy applies to all individuals who use the school's ICT systems, both on and off-site. These include:

- **Staff**
- **Students**
- **Volunteers**
- **Parents/Guardians**
- **Contractors**
- **Community Users**

3. Roles and Responsibilities
3.1 Governing Body

The Governing Body is responsible for:

- Approving and reviewing the effectiveness of this policy.
- Receiving regular reports on online safety incidents.
- Appointing the Online Safety Leader and overseeing the policy's implementation.
- Reviewing incident logs and technical monitoring reports.

3.2 Online Safety Leader

- Leads the policy's implementation and ongoing review.
- Monitors online safety incident logs and filtering reports.
- Ensures staff receive appropriate training.
- Reports regularly to the Governing Body.

3.3 Principal

- Ensures the safety of all members of the school community, including online safety.
- Coordinates procedures for handling online safety incidents involving staff members.

3.4 Online Safety Coordinator

Head of Academics, is responsible for:

- Leading the online safety group.
- Reviewing and updating online safety policies.
- Providing training and advice for staff.
- Maintaining logs of online safety incidents and liaising with technical staff.
- Reporting regularly to the Governing Body.

3.5 IT Administrator & Facilities Manager

- Ensure the security and integrity of the school's network infrastructure.
- Implement and regularly update filtering and monitoring policies.
- Maintain password protection and access control systems.

3.6 Staff

- Familiarize themselves with the school's Online Safety Policy and Acceptable Use Policy (AUP).
- Report any online safety concerns.
- Communicate professionally with students and parents through official school systems.

3.7 Social Workers

- Monitor online safety issues related to child protection and safeguarding.
- Provide training to staff regarding online safety risks such as exposure to inappropriate content and grooming.

3.8 Students

- Follow the Student Acceptable Use Policy.

- Report incidents of cyberbullying or inappropriate content.
- Understand the importance of using digital technologies responsibly.

3.9 Parents/Guardians

- Support the school's online safety initiatives and educate their children on appropriate online behavior.
- Participate in awareness activities such as parents' meetings and digital safety campaigns.

3.10 Contractors/Visitors

- Adhere to the school's online safety protocols.
- Report any concerns to the designated safeguarding lead or online safety coordinator.

4. Policy Statements
4.1 Use of Digital Images and Video

The school encourages the use of digital images and videos for educational purposes but requires strict adherence to policies to minimize potential risks:

- **Student and Staff Education**: Teachers must educate students about the risks of publishing digital images online, such as exposure to cyberbullying.
- **Parental Consent**: Parents/guardians are welcome to capture personal images of their children at school events but should refrain from publishing these images on social media.
- **Staff Guidelines**: Only school equipment should be used to capture images for educational purposes. Personal devices should not be used.
- **Privacy and Safety**: Students must not take, share, or distribute images of others without consent.
- **Publishing Images**: Any photographs shared publicly (e.g., on the school website) should comply with good practice, ensuring student privacy by avoiding full names or sensitive information.
- **Written Consent**: Written consent from parents/guardians is required before publishing images of students on the website.

4.2 Data Protection

Crown Private School is committed to safeguarding personal data in accordance with UAE Federal Law and international best practices:

- **Data Minimization**: Only essential personal data will be collected, processed, and retained for as long as necessary.
- **Accuracy and Access**: The school ensures that all personal data is accurate and updated. Data subjects have rights to access their personal data.

- **Data Security**: Staff must use password-protected devices and encrypt personal data when transferring it.
- **Incident Management**: Procedures are in place for reporting and managing data protection incidents.

4.3 Communications

The school uses a range of communication technologies to support learning. Staff and students must adhere to these best practices:

- **Email Communication**: All communications should be conducted via the official school email service, which is monitored for security.
- **Inappropriate Communications**: Any uncomfortable, offensive, or threatening communications should be reported immediately to the Online Safety Coordinator.
- **Professional Tone**: All digital communications between staff and students or parents must be professional and appropriate.

4.4 Social Media - Protecting Professional Identity

Staff must follow guidelines to protect both personal and school identities online:

- **Avoid Personal References**: Staff should not refer to students, parents, or school staff on personal social media.
- **Security Settings**: Staff should regularly check and update security settings on their personal social media profiles to protect personal information.
- **School Social Media Use**: The Online Safety Coordinator will review the school's use of social media to ensure compliance with school policies.

5. Education and Training
5.1 Staff and Volunteers

- **Induction Training**: All new staff will receive online safety training as part of their induction program.
- **Ongoing Training**: The Online Safety Coordinator will provide regular updates on new risks, technical tools, and legal requirements.
- **External Training**: The Online Safety Coordinator will attend external training events and share relevant information with staff.

5.2 Governing Body

The Governing Body will undergo online safety training, particularly for those involved in technology, online safety, and child protection matters.

6. Technical Infrastructure and Security

6.1 Network and Device Security

- The school will ensure that its network infrastructure is secure, regularly updated, and protected against misuse and cyberattacks.
- Password protection and access controls will be enforced across all systems.

6.2 Filtering and Monitoring

- The school will implement filtering measures to block access to harmful content and monitor the network for misuse.
- Filtering systems will be regularly updated to ensure effectiveness.

6.3 Bring Your Own Device (BYOD) Policy

- The BYOD policy ensures that personal devices used by students and staff are secure and comply with school protocols.
- Devices will be subject to the school's filtering system, and all users will be required to follow the Acceptable Use Agreement.

7. Monitoring and Review

- **Incident Logs**: All online safety incidents will be logged and reviewed regularly to inform improvements in policies and practices.
- **Feedback**: The school will conduct surveys and gather feedback to assess the effectiveness of the policy.
- **Policy Review**: This policy will be reviewed annually or sooner in response to significant technological developments or incidents.

8. Conclusion

Crown Private School is committed to providing a safe and secure digital environment for all its members. By adhering to the guidelines in this policy, we aim to foster responsible and informed use of digital technologies and minimize online risks.