CROWN PRIVATE SCHOOL
مدرسة كراون الخاصة
British Curriculum المنهاج البريطاني

FILTERING POLICY

PROCESS NAME:	Filtering 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 Online Safety Policy

1. Introduction

This policy sets out the principles to maintain and support research, teaching, and other business activities while protecting users, networks, and computers from unwanted network traffic and illegal content. It aims to comply with UAE Data and Privacy Protection laws, ensuring that Crown Private School provides a secure and controlled online environment.

2. Scope

This policy applies to all users of the Crown Private School network, including:

- **Employees**
- **Students**
- **Contractors**
- **Interns**
- **Casual Workers**
- **Agency Staff**
- **Partners**
- **Parents/Guardians**
- **Visitors**

It covers all communications between the school's networks and the internet, including web browsing, applications, instant messaging, file transfer, file sharing, and other internet protocols.

3. Policy Overview

Crown Private School uses a combination of firewall and web filtering technologies to prevent access to harmful or illegal content via its network. In line with UAE laws on data protection and internet access management (IAM), the school enforces this content filtering policy on all devices connected to its network with internet access.

- **Content Classification System**: The school's firewall vendor provides a content classification system that automatically blocks access to websites based on specific categories, such as:
  - **Adult Content**
  - **Hacking**
  - **Extremism**
  - **Fraud**

These categories are maintained and updated regularly by the firewall vendor to ensure compliance with national regulations.

4. Categories Blocked Under This Policy

4.1 Prohibited Domains

Access to domains that violate UAE laws, such as those related to pornography, human trafficking, or promoting illegal behaviors, will be blocked.

4.2 Impersonation, Fraud, and Phishing

Sites that engage in deceptive practices, such as phishing, fraud, or embezzlement, are blocked.

4.3 Insult, Slander, and Defamation

Any content that includes insult, slander, or defamation will be blocked to protect individual rights and maintain public order.

4.4 Invasion of Privacy

Sites that facilitate illegal activities such as phone tapping, espionage, or publishing private information without consent will be blocked.

4.5 Offenses Against the UAE and Public Order

Content that ridicules, abuses, or promotes harmful activities against UAE leaders, laws, and national symbols will be blocked.

4.6 Supporting Criminal Acts and Skills

Sites that promote or facilitate criminal activities (e.g., theft, fraud, murder, blackmail) will be blocked.

4.7 Drugs

Sites promoting drug-related content, including the sale or distribution of illegal substances, will be blocked.

4.8 Medical and Pharmaceutical Violations

Sites violating medical laws, such as those promoting unauthorized pharmaceutical products or violating medical advertising laws, will be blocked.

4.9 Infringement of Intellectual Property Rights

Sites that infringe on intellectual property rights, including those distributing pirated media or software, will be blocked.

4.10 Discrimination, Racism, and Contempt of Religion

Sites that contain or promote offensive or discriminatory content related to religion, race, or culture will be blocked.

4.11 Viruses and Malicious Programs

Sites that distribute viruses, malware, or hacking tools will be blocked to protect the network.

4.12 Promotion of Prohibited Commodities and Services

Sites that promote illegal or prohibited goods and services, such as counterfeit money, gambling, firearms, and drugs, will be blocked.

4.13 Gambling

Access to gambling-related sites will be blocked.

4.14 Terrorism

Sites related to terrorist organizations, or that promote terrorism or violent activities, will be blocked.

4.15 Illegal Activities

Sites promoting illegal activities, such as unauthorized donation collections or unlicensed trading, will be blocked.

4.16 Judicial Orders

Content that is blocked by order from the judicial authority or public prosecution will be blocked, in compliance with UAE laws.

---

5. Reporting System / Route

Whitelisting Requests:

- Whitelisting requests can be made via two channels:
    1. **Email**: share the URL of the 'Blocked Page' to IT Helpdesk to submit a request for whitelisting.
    2. **Call**: Users can contact the IT Helpdesk (Extn: 211).

Whitelisting Process:

- All whitelisting requests should be supported by appropriate evidence, including approvals from relevant staff members for research purposes.
- **Security Check**: All requests will be checked for malware and reviewed to ensure they are not miscategorized by the firewall vendor.
- **Final Decision**: The Senior Leadership Team (or nominee) will review the request, considering the purpose and legitimacy of the site. If the request is approved, IT Coordinator will take the necessary action.

---

6. Roles & Responsibilities

6.1 Online Safety Coordinator

The Online Safety Coordinator is responsible for ensuring that this policy is implemented and followed. They will collaborate with IT Administrators to review and approve any requests for whitelisting.

6.2 IT Administrators

IT Administrators are responsible for managing the network's firewall, implementing web filtering, and monitoring network traffic to ensure compliance with this policy.

6.3 Senior Leadership Team

The Senior Leadership Team will review whitelisting requests and ensure the final decision is made in alignment with the policy's objectives.

---

7. Relationship with Existing Policies

This Filtering Policy forms an integral part of the Crown Private School Online Safety Policy. It should be read in conjunction with the **CPS Acceptable Use Policy**.

---

8. Monitoring and Breach of Filtering Policy

Step 1: The IT Administrator will monitor and analyze network traffic from the firewall on a daily basis.

Step 2: Alerts will be generated by the firewall for:

- Accessing blocked/filtered content
- Intrusion attempts
- Heavy bandwidth usage

Step 3: Breach reports will be shared with the Online Safety Coordinator and Online Safety Leader.

Step 4: The IT Administrator will investigate any breach and report findings to the Online Safety Coordinator (Vice Principal) and Online Safety Leader (Principal).

Step 5: Further action will be taken based on the severity of the breach.

Step 6: A detailed report with conclusions will be maintained by the IT Administrator.

---

9. Conclusion

Crown Private School is committed to providing a safe and secure online environment for all users. By adhering to this Filtering Policy, the school aims to protect its network, prevent access to harmful content, and ensure compliance with UAE laws.