



## Firewall Policy - including explanation and consequences

### Introduction

This policy outlines the use of the firewall and internet filtering at Jeanne d'Arc British International School in order to ensure a safe, secure but productive online environment for students from Stage 2 to Stage 12.

The policy supports the educational mission while protecting students from inappropriate content and cyber threats.

This policy should be read in conjunction with the E-Safety Policy

### How a Firewall Works

A firewall is a security system, either hardware, software, or both, that acts as a gatekeeper between the school's internal network and the internet. It monitors all incoming and outgoing internet traffic and enforces rules about what types of connections are allowed or blocked.

- The firewall inspects web requests and blocks access to websites or online content that violate the school's policies, such as sites with inappropriate content, violence, or other material unsuitable for children.
- It uses techniques like URL filtering (blocking specific web addresses), category filtering (blocking entire types of websites like gaming or social media), and application control (managing which apps or services can be accessed).
- The firewall also inspects encrypted traffic (HTTPS) to ensure harmful content is not bypassing filters.
- By doing this, the firewall protects students from exposure to inappropriate material and helps prevent malware or cyberattacks from entering the school network.

### Purpose of the Firewall Policy

- To comply with safety requirements as stated in the Keeping Children Safe in Education (2024) statutory guidance which requires schools to limit children's exposure to risks from the school's IT systems.
- By blocking harmful or illegal content and creating user policies that address bring-your-own-device terms of use which are key to KCSIE compliance.
- To create a safe and distraction-free learning environment by restricting access to inappropriate or non-educational websites.

- To protect the school's network infrastructure from cyber threats and unauthorised access.

### **Internet Use and Restrictions**

- Students are only allowed to access websites and online resources that support their educational activities.
- Access to websites containing inappropriate content such as violence, hate speech, gambling, or other unsuitable material is strictly prohibited.
- Social media, gaming, and entertainment websites are restricted during school hours to minimise distractions but may be accessible during designated times or for educational purposes as approved by staff.
- The firewall will enforce these restrictions in real time, and any attempts to bypass the firewall or access blocked content will be logged and reviewed.

### **Consequences of Using Improper Sites at School**

Students who attempt to access or use improper websites or online content will face disciplinary actions consistent with the school's Acceptable Use Policy which involves meeting with parents and possibly not being permitted to bring a device to school.

Persistent attempts to access or use improper websites or online content may result in suspension and even expulsion in extreme cases.

### **Responsibilities**

- **Students** must use the internet responsibly, following the school's rules and respecting the firewall restrictions.
- **Teachers and Staff** will monitor student internet use during classes and report any violations.
- **The IT Department** will manage the firewall settings, update filtering rules, and ensure the system is functioning properly to protect students and the network.

The firewall system installed is the FortiGate FortiWiFi 60F Series

### **Policy Review**

This policy will be reviewed annually to adapt to new technologies, threats, and educational needs.

The most recent review was May 2025