THE WALLACE HIGH SCHOOL
CYBER SECURITY POLICY

Adopted by Board of Governors on: ***16 December 2024***

To be reviewed: ***December 2025***

Introduction

This Cyber Security Policy outlines the measures and guidelines that The Wallace High School implements to safeguard its digital assets and protect against cyber threats. The policy aligns with best practices recommended by the National Cyber Security Centre (NCSC) and aims to ensure the confidentiality, integrity, and availability of school information systems and data.

Scope

This policy applies to all staff, students, contractors, and any other individuals who have access to The Wallace High School's digital resources and networks, including those working remotely or from home.

Types of Cyber Attack

Below is a list of the main categories of cyber-attack. This list is not exhaustive and will be updated as new threats emerge:

Phishing
Phishing attacks attempt to deceive individuals into revealing sensitive information or performing actions that compromise security. A targeted phishing attack could be used to gain access to a user's account that has important information (such as a member of the Leadership Team) or a user with administrative privileges to the network.

Phishing is usually in the form of an email sent to either a list of users or an individual. The attacker would craft an email to disguise it to seem normal, with either malware attached that looks like a normal document, or links to fake but legitimate looking web pages with the intent of harvesting sensitive data from the user.

To mitigate the risk of phishing attacks, The Wallace High School will:

a) Conduct regular awareness training sessions to educate staff and students about recognising and reporting phishing attempts.
b) Implement email filters and firewalls to minimise the delivery of phishing emails, including SPK, DKIM and DMARC and spam filtering provided by Google.
c) Encourage the use of strong email security practices, such as verifying sender authenticity and exercising caution when clicking on links or downloading attachments.

Ransomware
Ransomware is a type of malware that encrypts data and demands payment for its release. A ransomware attack usually happens when a user opens a malware file or link on a network connected computer. The malware file has specific scripts to identify and encrypt the files in the target area. Ransomware could be used to

encrypt a school's financial and contact data so that the school would not be able to access it.

The Wallace High School will take the following measures to prevent and respond to ransomware attacks:

a) Regularly update and patch operating systems, software, anti-virus and applications to address known vulnerabilities and to ensure effective detection and removal of malicious attachments.
b) Implement robust backup and disaster recovery mechanisms to ensure the availability of critical data.
c) Conduct periodic security assessments to identify potential vulnerabilities and improve incident response procedures.
d) Maintain offline or off-site backups to mitigate the risk of ransomware affecting backup systems.
e) Implement robust email filtering systems to detect and block emails with suspicious attachments.
f) Educate staff and students about the risks associated with opening attachments from unknown or untrusted sources.

Password Attacks and Brute Force

Password attacks involve unauthorised attempts to gain access to user accounts through methods such as brute forcing or password guessing.

The Wallace High School will implement the following measures to strengthen password security:

a) Enforce the use of complex passwords and multi-factor authentication (MFA) where feasible. MFA is enforced on all staff email accounts.
b) Regularly educate staff and students on password security best practices and the importance of unique passwords.
c) Monitor user accounts for suspicious activity, such as multiple failed login attempts or unusual login patterns.
d) Promptly disable or reset compromised accounts to prevent further unauthorised access.

Denial of Service (DoS)

Denial of Service attacks aim to disrupt the availability of networks, systems, or services. The Wallace High School will employ the following strategies to mitigate the impact of DoS attacks:

a) Deploy network and system monitoring tools to identify abnormal traffic patterns and potential DoS attacks.
b) Implement load balancing and redundancy mechanisms to distribute traffic and maintain service availability for critical systems.

Internet security and filtering

The Wallace High School filters access to the Internet in the interest of security and pupil safety. Filtering prevents access to inappropriate sites and can prevent inadvertent access to dangerous site with malicious software.

In addition, the firewall will prevent unauthorised access to system from outside by identifying and blocking malicious traffic.

Working from Home

Given the increasing prevalence of remote work, The Wallace High School recognises the need to address cyber security concerns for individuals working from home.

The following guidelines will apply:

a) Provide secure remote access mechanisms, such as Virtual Private Networks (VPNs), to ensure encrypted and authenticated connections.
b) Educate staff and students on best practices for securing home networks, including regular patching and use of strong Wi-Fi passwords.
c) Encourage the use of school-provided devices or implement bring-your-own-device (BYOD) policies with appropriate security measures.

USB Pens

The school does not recommend the use of USB pen drives or portable hard drives. If these devices must be used, they MUST be encrypted with a secure password. Students and staff are recommended to use other means of transferring data such as email or Google Drive as these methods are considered to be more secure.

Compliance and Monitoring

The Wallace High School is committed to regularly reviewing and updating this Cyber Security Policy to adapt to emerging threats and technologies. The school will conduct periodic audits and assessments to ensure compliance with this policy and may take appropriate actions in the event of policy violations.

Reporting Incidents

All staff, students, and stakeholders are encouraged to promptly report any suspected or actual cyber security incidents to the designated contact point, ensuring a swift response and effective resolution.

Policy Review

This Cyber Security Policy will be reviewed annually or as deemed necessary to ensure its continued relevance and effectiveness in safeguarding The Wallace High School's digital assets and information systems.