Educational Excellence *for* Life and Leadership

Digital Safeguarding Policy

HARROW INTERNATIONAL SCHOOL HONG KONG

1. Introduction

Harrow International School Hong Kong is committed to providing a safe and secure learning environment for all pupils, both in the physical classroom and in the digital world. This Digital Safeguarding Policy sets out to create a safe and secure digital environment for all members of the school community and to promote responsible digital citizenship.

2. Key Principles

- **Pupil Safety**: The safety and wellbeing of pupils is our top priority.
- **Positive Digital Culture**: We promote a positive and responsible digital culture that fosters respect and inclusion, in line with the School's values and social vision.
- **Digital Literacy Education**: We educate pupils about online risks, cyberbullying, privacy, and responsible online behaviour.
- **Incident Reporting**: We have clear procedures for reporting and responding to online incidents.
- **Collaboration**: We work collaboratively with parents and guardians to ensure online safety.

The key principles of our approach are outlined on the Digital Safeguarding Policy Infographic.

3. Safeguarding Measures

To ensure a safe and secure digital learning environment, Harrow International School Hong Kong has implemented a comprehensive set of safeguarding measures. These measures include a programme of digital literacy education, technological solutions, and policies to protect pupils from online risks and promote responsible digital citizenship.

3.1 Technology (Mobile Device policy)

- **Apple Classroom:** Apple Classroom empowers teachers by providing a platform to monitor class activity summaries, enabling them to maintain an overview of pupil engagement as well as supporting online safety through, so called, *physical monitoring*. Additionally, its ability to monitor pupil activity in real-time aids in safeguarding by allowing teachers to quickly identify and address any inappropriate or risky online behaviour, ensuring pupils remain focused and safe during their digital learning experiences in class.

- **LightSpeed Safeguarding Software**: This tool integrates content filtering, monitoring and machine learning scanning to create a secure digital environment by effectively monitoring and managing online activities. It plays a crucial role in preventing risky online behaviours and ensures that users can only access safe and approved online resources, reducing the risk of exposure to malicious sites or phishing attempts that could compromise data security. LightSpeed is installed on all registered pupil-owned MacBooks (Senior School) and iPads (Pre-Prep and Prep School) as well as school-owned devices. This comprehensive coverage ensures consistent protection and monitoring across all platforms.

    - **LightSpeed Filter:** LightSpeed filter blocks websites and applications that are not appropriate for pupils to be using. This includes traffic through applications, VPNs and tethering to 4G/5G hotspots.

- **LightSpeed Monitor:** LightSpeed monitor provides comprehensive reporting on pupils' online activity including logging when attempts are made to access sites that have been blocked.

- **LightSpeed Alert**: LightSpeed Alert scans online content for warning indicators of self-harm, cyberbullying, or violence which are relayed to pastoral leaders and the School's DSLs enabling timely intervention. In this way it provides active monitoring in the cases where the risk is highest.

- **Device MAC Address Filtering**: Only devices enrolled in the School's MDM, Jamf Pro are able to access the internet through the School's WiFi network. Filtering by device in this way ensures only approved devices, equipped with the required software, can access the school's Wi-Fi. This measure is in place to support compliance, especially in cases where pupils' devices are replaced.

- **Firewall**: The school implements a robust firewall system that actively monitors and blocks access to inappropriate, malicious, or non-educational websites. This includes content related to gaming, social media, adult content, proxy servers, and other potentially harmful materials. The system generates comprehensive reports detailing attempted access to blocked websites, which are reviewed by the ICT department and the DSL. The ICT department reviews anonymised and aggregated data to identify patterns and adjust filtering policies as needed and the DSL reviews concerns related to individual pupils. This proactive approach ensures pupils maintain focus on educational content while protecting them from online threats. The firewall's intelligent categorisation system is regularly and automatically updated to respond to new online threats and maintain alignment with the school's educational objectives.

- **Disabling Admin Access pupil-owned devices through the School's MDM, Jamf Pro:** To prevent pupils from installing games or other distracting applications, admin access is disabled on all Year 3 - Year 9 MacBooks and iPads. Additionally, the Apple Store is hidden on iPads. Parents have the option to set up a Family Sharing account on their child's device. Through this setup, they can manage apps and programs installed on the device while ensuring it aligns with the School's learning objectives.

- **Regular Audits**: The school conducts regular (at least annual) audits of technological tools to ensure they remain effective and up to date.

- **Data Privacy Compliance**: The school ensures compliance with local data protection regulations, by regularly reviewing data handling procedures.

- **Device expected usage and software check-in reports:** IT monitor the usage of devices to ensure compliance with the installation and maintenance of the safeguarding software. For example, if a pupil manages to uninstall Jamf, it will generate an alert to the IT department. These reports and alerts trigger investigations with the support of the Pastoral team. Refer to Appendix 4, Digital Safeguarding non-compliance protocol for details.

3.2. Timed Wi-Fi Access in Boarding Houses

To promote healthy online habits, encourage focused learning, and ensure adequate rest, Wi-Fi access in boarding houses follows a schedule. Specifically, WiFi access switches off at night. This measure helps to balance digital engagement with offline activities and promotes a healthy sleep schedule.

- **Prep Houses (Years 6-8):** Wi-Fi is turned off from 8:30 pm to 7:30 am.
- **Senior Houses (Years 9-11):** Wi-Fi is turned off from 10:30 pm to 6:30 am.
- **Sixth Form (Years 12-13):** Wi-Fi is turned off from 11:00 pm to 6:00 am.
  This later cutoff time accommodates the older pupils' academic demands and allows for a slightly extended evening for personal activities.

3.3 Filtering and Monitoring

At Harrow Hong Kong, we use filtering software to restrict access to inappropriate content and monitor online activity on pupil devices to ensure responsible and safe use. The Pupil ICT Code of Conduct defines expected online behaviours, and all pupils and parents/guardians must agree to it before accessing school networks.

Monitoring takes two forms: logging of attempted access to filtered sites through both the LightSpeed filter and the network Firewall and the active monitoring for warning indicators of harm through LightSpeed.

Updating filtering rules: If a website is mistakenly blocked, both pupils and staff can report this to the school's ICT department. They have the option either to send an email to askit@harrowschool.hk or to fill out a Microsoft Form: here. This ensures swift resolution of access issues, maintaining smooth and uninterrupted access to online resources.

Any changes to the monitoring system go through an approval process and are logged, enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes.

To ensure that our filtering rules are appropriate they are reviewed and updated regularly. The UK Safer Internet Centre endorsed Test filtering utility is used at least annually to review the School's filtering rules. See Appendix 8.

3.4 Reporting and Monitoring of Online Activity

Harrow Hong Kong have enhanced reporting and monitoring protocols for online activity. These protocols ensure that data collected through the firewall and LightSpeed systems is reviewed and used effectively and responsibly to maintain the safety and well-being of pupils while complying with the Personal Data (Privacy) Ordinance (PDPO).

3.4.1 Firewall Reporting and Review by the Pastoral Team

The school's firewall system generates detailed reports on attempted access to blocked websites and other restricted online activities. These reports are reviewed by the Pastoral Team under the following guidelines:

a. Data Scope:
- Reports will include anonymized or aggregated data where possible, focusing on patterns of inappropriate access attempts.
- For identified incidents, specific user data (e.g., device identifiers, timestamps, and URLs) may be accessed to investigate breaches of the Pupil ICT Code of Conduct.

b. Access Control:
- Firewall reports are sent via secure access links, accessible only to authorised members of the Pastoral Team.

c. Purpose:
- To identify trends in inappropriate online behaviour and adjust policies and education accordingly.
- To address individual incidents where pupils attempt to access harmful or inappropriate content.

d. Frequency:
- The ICT department provide weekly summaries of firewall activity to the Pastoral Team.
- Real-time alerts for critical incidents (e.g., attempts to access adult content or malicious websites) will be escalated immediately.

3.4.2 LightSpeed Reporting and Review by the Pastoral Team

LightSpeed provides advanced monitoring capabilities, including alerts for risky online behaviours such as self-harm, cyberbullying, or violence. The following protocols govern the use of this data:

a. Data Scope:
- LightSpeed generates alerts based on predefined risk indicators, encompassing flagged keywords, unusual browsing activity, screen capture reports, and monitor activity logs.

- When monitoring is turned on, the system collects web activity data including URL access records, browsing duration, website categories, download activities, search queries, bandwidth usage, time-stamped web sessions, and browser information.
- All alerts and reports contain essential identifiers such as device information, user profiles, timestamps, and flagged content, alongside screen monitoring data that includes a screenshot capture, activity timeline and application usage logs.

To maintain compliance with Hong Kong's Personal Data (Privacy) Ordinance (PDPO), the system adheres to specific data retention periods: web activity logs are kept for 90 days, screen captures for 30 days, real-time monitoring data for 60 days, and alert records for 90 days.

b. Pastoral Leaders' monitoring responsibilities:
- Access Attempt Analysis – Review frequent attempts to access blocked material, monitor patterns of attempted circumvention of filtering systems and track repeated access attempts to specific categories of concern.
- High-Risk Content Monitoring - Review attempts to access harmful or dangerous material, monitor searches related to self-harm, violence, or extremism and track access attempts to age-inappropriate content.
- Behavioural Pattern Analysis - Review time spent searching and browsing patterns, monitor unusual timing of online activity and track changes in typical usage patterns that may indicate concerns.
- Policy Compliance - Ensure adherence to acceptable use policies, monitor compliance with school device policies and track appropriate use of educational resources

c. Review and Response Frequency:
- The LightSpeed Portal provide summaries of LightSpeed alerts to the Pastoral Team (Year Leaders, HMs and the DSL).
- Critical alerts are automatically sent to the DSL and pastoral leader within one hour of detection.
- High priority alerts must be reviewed daily and receive a same-day response.
- For further details refer to Appendix 3.
- Standard filter reports are to be reviewed weekly.
- Trend analysis should be undertaken periodically.

d. Access Control:
- Access to LightSpeed reports is restricted to the Pastoral Team.
- Alerts specific to safeguarding concerns are sent directly to the Designated Safeguarding Lead (DSL) for immediate attention.
- All access to LightSpeed data is via restricted permissions, password protected and logged, with periodic audits conducted to ensure compliance with access policies.

e. Purpose:
- To enable timely interventions for safeguarding concerns, such as identifying pupils at risk of harm.
- To support the school's behaviour policies by addressing inappropriate online behaviour.
- To enhance educational outcomes by ensuring a focused and secure digital learning environment.

3.5 Access to Data and Roles

In accordance with the PDPO and the principles of data minimization and purpose limitation, access to firewall and LightSpeed data is strictly governed by role-based permissions:

1. Roles with Access:
- ICT Pastoral Liaison: Responsible for managing and maintaining the firewall and LightSpeed systems and generating reports. The ICT Pastoral Liaison does not have access to pupil data but facilitates the generation and dissemination of reports for the Pastoral Team.
- A pupil's Pastoral Leader (House parent in the Upper School and Year Leader in the Lower School): Authorized to review reports and alerts related to pupil safeguarding and behaviour management.
- The Designated Safeguarding Lead (DSL) is responsible for:
    - Monitoring and reviewing automated safeguarding alerts generated by LightSpeed across all Year groups
    - Managing the investigation process of any flagged safeguarding concerns

- Senior Leadership Team (SLT): May access aggregated and anonymized data for strategic decision-making and policy updates.

2. Data Categories:
- Aggregated Data: Used for trend analysis and policy adjustments (e.g., identifying patterns of blocked website access).
- Identifiable Data: Accessed only when investigating specific incidents, behavioural or safeguarding concerns.

3. Access Protocols:
- All access to data is logged and subject to regular audits.
- Staff with access must complete annual training on data protection and safeguarding protocols.
- Unauthorized access or misuse of data will result in disciplinary action in accordance with the school's policies.

3.6 Uses of Data

Data collected through the firewall and LightSpeed systems is used exclusively for the following purposes, in compliance with the PDPO:

1. Safeguarding Pupils:
    a. Detecting and responding to risks such as cyberbullying, self-harm, or exposure to harmful content.
    b. Supporting the DSL and Pastoral Team in providing timely interventions.
2. Behaviour Management:
    a. Monitoring adherence to the Pupil ICT Code of Conduct.
    b. Addressing inappropriate online behaviour through the school's behaviour policies.
3. Policy Development:
    a. Identifying trends in online activity to inform updates to the Digital Safeguarding Policy and filtering rules.
    b. Enhancing the school's digital Literacy curriculum based on emerging risks.
4. Educational Support:
    a. Ensuring pupils remain focused on educational content during digital learning activities.
    b. Promoting a positive and secure digital learning environment.

3.7 Compliance with the Hong Kong PDPO

Harrow International School Hong Kong ensures that all data collection, storage, and processing activities comply with the PDPO by adhering to the following principles:

1. **Data Minimization**: Only data necessary for safeguarding, behaviour management, and educational purposes is collected.
2. **Purpose Limitation**: Data is used exclusively for the purposes outlined in this policy and is not shared with unauthorized parties.
3. **Transparency**: Pupils, parents, and staff are informed about the data collected through the firewall and LightSpeed systems and its intended uses.
4. **Security**: Data is stored securely, with access restricted to authorized personnel and protected by robust technical safeguards.
5. **Retention:** Data is retained only for as long as necessary to fulfil its intended purpose and is securely deleted thereafter.

3.8. Digital Literacy Education

Harrow Hong Kong ensures that all of our Pupils' education includes the digital knowledge and skills necessary to stay safe online, and safeguard their wellbeing. This is a component of the **Digital Literacy** curriculum and is taught through Computing lessons in the Lower School and a combination of Computer Science lessons and the

PSHE curriculum in the Upper School. The components taught align with the UK Government's Education for a Connected World framework and are detailed in the Digital Strategy Policy. Digital Safety guidance for pupils includes specific reference to the online threats posed by the '4Cs': content, contact, conduct, and commerce.

Parent Webinars: The school offers annual webinars for parents to help them understand some of the digital literacy skills necessary and what they can be doing at home to support their children.

3.9 Safeguarding and AI

Generative AI tools pose specific and significant safeguarding risks to pupil wellbeing including, but not limited to, exposure to harmful content including AI-generated child sexual abuse material (AI-CSAM), bullying, grooming, and harassment. In addition, the misuse of personal data can lead to privacy breaches, the creation of false or misleading information, and increased risks of cyber-attacks, fraud, and scams. Unauthorised use of copyrighted materials can lead to intellectual property issues, and the perpetuation or amplification of existing biases in AI systems can result in unfair treatment or discrimination.

We are committed to ensuring the safe and responsible use of AI technologies, and our measures are outlined in our AI Policy. These include:

- **The teaching of AI literacy** as part of the digital literacy curriculum
- **Generative AI tools are, by default, blocked** as part of the LightSpeed filtering rules in the Pre-Prep and Prep Schools
- **All generative AI applications undergo a thorough risk assessment** to evaluate their benefits and potential risks before being unblocked and/or used in the classroom, ensuring compliance with legal responsibilities such as data protection, child safety, and intellectual property laws.

3.10 Mobile Phones and unrestricted access to the internet

Mobile phones provide discrete, unsecured and unmonitored access to the internet and so the reduction of risk is a particular consideration of this policy. This risk is increased by the ability to use a mobile or personal portable 5G router to connect (tether) mobile devices (iPads or MacBooks) to the internet without going through our network filters. This policy addresses this in a number of ways:

- **Restrictions on mobile phone usage during school hours:** The carrying and use of mobile phones around campus is strictly limited.
- **Restrictions on mobile phone usage during trips:** Lower School and Prep School pupils should not use mobile phones unless with specific permission, this includes offsite activities such as SCAs and fixtures. Senior Pupils can use devices during journeys and official breaks. Overnight trips should adhere to the boarding mobile phone use policy below, or if the nature of the trip requires a phone-free environment is maintained. More details can be found in the Trips and Visits Policy.
- **Restrictions on use of tethering:** In order to ensure that online activity is safeguarded whilst at School. Tethering to mobile phones or portable 5G routers is prohibited and this is included in the Pupils ICT Code of Conduct, which pupils sign each year.
- **LightSpeed agent continues to protect on mobile broadband**: As software installed on the device, for MacBooks (Senior School) and supervised iPads (Pre-Prep and Prep School), LightSpeed continues to filter and monitor internet activity even when tethering to a mobile phone.
- **Spot checks through Jamf MDM**: The IT department generate automated reports at least three times a day on managed devices connecting to non-school networks. This information is used by the pastoral team to address non-compliance.
- **Restrictions on mobile phone usage and tethering for boarders during the evening:** The use of mobile phones for boarders in the evening is managed. Senior Boarders in Years 9 and 10 hand in their phones from 6.30pn-8.30pm during supper and Prep time. They are able to collect their phones at 8.30pm to contact parents until 8.45pm. All phones and devices are handed in by Year 9 and 10 from 8.45pm until 7.45am. For Year 11 phones and devices are handed in overnight from 9.30pm until 7.45am the following morning. In, the Prep Houses pupils have access to their phones between 5.30pm until 6pm. Phones for Year 6 and Year 7 are available for boarders to call parents between 7.30pm-7.45pm each evening. Year 8 boarders have access to their phones between 8.15pm-8.30pm. All phones and devices

are secured overnight until 7.30am the following morning This is supported by physical monitoring by the house pastoral team and IT tethering reports.

4. Incident Reporting and Response

4.1 Firewall and LightSpeed Reporting

Reports generated by the firewall and LightSpeed systems will be integrated into the school's incident response process as follows:

Reporting:

1. Critical alerts from LightSpeed (e.g., indicators of self-harm) are escalated immediately to the DSL.
2. Firewall incidents involving repeated attempts to access restricted content are flagged for investigation by the Pastoral Team.

4.2 Reporting by Pupils

- **Reporting**: Pupils are encouraged to report online safety concerns to trusted adults, such as teachers, HMs or the Designated Safeguarding Lead (DSL).
- **Anonymous Reporting**: The school provides a secure online form accessible via the school intranet for anonymous reporting of digital safety concerns which is directly routed to the DSL.

4.3 Digital Safety Response Protocol

The school deals with online incidents through its behaviour policies, which include investigative procedures, disciplinary measures, and support for pupils involved.

- The DSL leads investigations in collaboration with the ICT department and relevant staff.
- Disciplinary measures and support plans are implemented in accordance with the school's behaviour and safeguarding policies.

4.4 Response Timeliness

The school maintains strict response timelines for all reported incidents, categorized by severity level. Critical incidents (where there is a danger to life) require immediate attention and must be addressed within one hour of reporting, while other concerns are handled promptly and certainly within a 48-hour timeframe to ensure appropriate attention to all cases. Throughout the incident management process, relevant stakeholders receive regular status updates on the progress and resolution of reported issues. The effectiveness of these response protocols is reviewed monthly by the ICT department and senior management to maintain and improve service standards, ensuring optimal handling of all security and safety concerns.

4.5 Documentation

All incidents are documented, and data logs are retained for audit purposes in compliance with the PDPO.

5. Staff Responsibilities

- **Training**: All staff undergo training on digital safeguarding procedures and their role in promoting a safe online environment.
- **Monitoring and Reporting**: The Pastoral Team monitors pupil online activity and report any concerns to the DSL/DDSLs.
- **Modelling Responsible Behaviour**: Staff model responsible digital behaviour following the Staff IT Acceptable Use Policy (read and signed annually).
- **Communication with Parents**: The Pastoral Team regularly communicate with parents about online safety and provide guidance on how to address digital risks at home.

6. Parental Responsibilities

- **Communication**: Parents are encouraged to regularly discuss online safety with their children and establish clear expectations for responsible online behaviour.
- **Monitoring**: Parents are encouraged to monitor their children's online activities and ensure safe internet usage.
- **Collaboration**: Parents are urged to communicate concerns about their child's online safety and collaborate with the school to address these issues.
- **Resources**: The school provides resources for parents to stay informed about online safety issues, including links to reputable online safety websites and tools.

7. Review and Update

Harrow Hong Kong is committed to ensuring this policy remains effective, relevant, and aligned with advancements in technology, emerging online threats, and evolving safeguarding needs. The review process is designed to foster continuous improvement through collaboration and feedback from the school community.

7.1 Regular Review and Consultation

- **Annual Review**: This policy will undergo an annual review to ensure its alignment with the latest safeguarding practices, technological developments, and compliance with Hong Kong's Personal Data (Privacy) Ordinance (PDPO).
- **Stakeholder Consultation**:
  - Feedback will be actively sought from key stakeholders, including staff, pupils, parents, and governors, to ensure the policy reflects the diverse needs of the school community.
  - The consultation process may include surveys, workshops, focus groups, and informal discussions to gather valuable insights and suggestions.
- **Incident Data Analysis**: Data from firewall and LightSpeed reporting systems, as well as incident logs, will be analysed to identify trends, evaluate the effectiveness of current measures, and address any recurring issues.

7.2 Effectiveness of Reporting Protocols

- The effectiveness of firewall and LightSpeed reporting protocols will be specifically reviewed during the annual policy evaluation.
- Feedback from the ICT department, Pastoral Team, and Designated Safeguarding Lead (DSL) will be used to assess and enhance the efficiency of monitoring, reporting, and response processes.
- Recommendations for improvements will be implemented promptly to maintain a robust safeguarding framework.

7.3 Policy Accessibility

- A summary of key safeguarding measures, including reporting protocols and digital literacy guidelines, are provided on the school website to ensure clarity and understanding.

7.4 Continuous Feedback Mechanism

- Feedback mechanisms allow stakeholders to provide ongoing input on the policy.
- Feedback will be reviewed regularly by the DSL and ICT department to ensure timely updates and improvements.
- Our digital safeguarding policy maintains effectiveness through structured feedback channels that enable stakeholder participation and timely improvements.

7.5 Community Engagement

- Termly PGCG meetings and House rep meetings for parents, as well as parent webinars and information evenings
- Student Council meetings, Pupil Digital Prefects and House digital reps
- Student voice through Tutor time and Pupil Digital Prefects
- Staff consultation in departmental meetings

7.6 Dynamic Updates

- The policy will be updated as needed to address:
- New online risks or safeguarding challenges.
- Changes in local regulations, such as updates to the PDPO.
- Technological advancements or the adoption of new safeguarding tools.
- Interim updates, if required, will be communicated to stakeholders promptly through official channels, including email notifications and the school website.

7.7 Transparency and Accountability

- All updates to the policy will be documented, with a summary of changes provided to stakeholders for transparency.
- The Senior Leadership Team (SLT) will oversee the review process to ensure accountability and alignment with the school's safeguarding objectives.

7.8 Use of mobile phones in the Early Years Centre

Mobile phones must not be used anywhere within the Early Years Centre in the presence of children (unless in the case of emergency).
Only digital devices owned by the school should be used to take photos and / or videos of pupils and their learning.

8. Appendices

- **Appendix 1**: Pupil ICT Code of Conduct
- **Appendix 2**: Staff ICT Acceptable Use Agreement
- **Appendix 3**: Safeguarding Alert protocol
- **Appendix 4**: Digital safeguarding non-compliance protocol
- **Appendix 5**: Digital Safety Response Protocols
- **Appendix 6**: Resources for Parents and Guardians (e.g., links to websites on online safety)
- **Appendix 7**: Glossary of Terms
- **Appendix 8**: Lightspeed configuration settings
- **Appendix 9**: Data safeguarding and Retention
- **Appendix 10**: Test Filtering Results

Reviewed: September 2025
Next Review: August 2026
Owner: Assistant Head (Digital Strategy, Assessment and Tracking)
Version: 2

Appendix 1: PUPIL ICT CODE OF CONDUCT (2024/25) [Upper School]

Linked here: PUPIL ICT CODE OF CONDUCT 2025-26

HARROW INTERNATIONAL SCHOOL HONG KONG

LOWER SCHOOL PUPIL DIGITAL CODE OF CONDUCT 2025-26

The School has a duty of care to ensure that each pupil at Harrow International School Hong Kong uses digital devices, the internet and communication devices safely and responsibly. Before using devices, all pupils are required to read, understand and sign this Code of Conduct. This applies to use of any devices which are connected to the School network, including iPads, MacBooks and other digital devices.

1. Pupils must never use another person's accounts or allow their own accounts to be used by another person.
2. Pupils should not send messages to each other over the internet, or by any other means, unless directed to do so by the teacher.
3. Pupils should not share any personal information, such as text or images, about the School or any individuals in it without permission.
4. Pupils should not attempt to access, send or store any inappropriate information, including images.
5. When using devices, including iPads, all pupils must follow the iPad Golden Rules, as displayed below and in classrooms.

If one of the above agreements is not fulfilled, the teacher has the right to restrict a pupil's access to their device.

I have read and understand the Lower School Digital Code of Conduct and agree to always follow this.

Signed by Pupil: _____

Date:_____

Appendix 2: STAFF ICT ACCEPTABLE USE AGREEMENT (2024/25)

This document sets out the security, administration and internal rules, which all members of staff at Harrow International School Hong Kong should observe when communicating electronically using any device or when using the School's ICT facilities. All members of staff should pay close attention to the terms of this Policy in order to minimise potential difficulties to themselves, pupils and the School, which may arise as a result of misuse of email or Internet facilities. This Policy applies to all employees of the School, as well as resident family members of employees, or any other guests who use School ICT facilities.

The School network is available for use by the whole School community, including academic and educational support staff, pupils, parents and visitors, and the School has a duty of care to ensure that each user at Harrow Hong Kong uses computer equipment and the Internet, as well as mobile phones and other communication devices responsibly. Users should expect their computer use on the School's network to be monitored, although this will be proportionate, i.e. only so far as is necessary and in such a way that the potential intrusion on privacy is limited. All users are expected to use the School ICT systems, resources and associated applications in activities that support the vision statement, goals and objectives of the School. ICT resources must, therefore, not be used for any illegal or unethical purpose and recreational or personal use should be minimised. Equally, users should not engage in any activity that may disrupt the effective operation of the network.

1. School Property

1.1 The School acknowledges and welcomes the creativity of staff in the production and storage of materials to support teaching, learning and administration. It is important to note that, according to the letter of the law, files and email messages created and stored on the School network by employees, contractors and residents in the performance of their normal duties technically remain the property of the School. In any question regarding copyright and intellectual property, members of staff are encouraged to seek advice from the Head.

1.2 Subject to the further provisions outlined in this Policy, files and email messages created and stored on the School network by employees, contractors and residents for their private and personal use remain the property of the creator.

2. Monitoring

2.1 The School's computer network is a business and educational tool to be used primarily for business or educational purposes. Members of staff, therefore, have a responsibility to use these resources in an appropriate, professional and lawful manner.

2.2 All messages and files on the School's system will be treated as education or business related, and may be monitored. Accordingly, members of staff should not expect any information or document transmitted or stored on the School's computer network to be entirely private.

2.3 Members of staff should also be aware that the School maintains systems that automatically monitor and filter use of the Internet, both during and outside working hours, including the sites and content that members of staff visit and the length of time they spend using the Internet.

2.4 Members of staff should structure their email in recognition of the fact that the School may, if concerned about possible misuse, need to examine its contents.

2.5 Emails will be archived by the School as it considers appropriate and to comply with statutory requirements.

3. Personal Use

3.1 Members of staff are permitted to use the Internet and email facilities via the School network to send and receive personal messages, provided that such use is kept to a minimum and does not interfere with the performance of their work duties.

3.2 However, any use of the School network for personal purposes is still subject to the same terms & conditions as otherwise described in this Policy, regardless of whether it is marked private or confidential.

3.3 In the case of shared IT facilities, members of staff are expected to respect the needs of their colleagues and use the computer resources in a timely and efficient manner.

3.4 Excessive or inappropriate use of email or Internet facilities for personal reasons during working hours may lead to disciplinary action. For instance, members of staff should not download large video/audio files for personal use, nor large quantities of images, nor download or install computer programs without the consent of the Director of ICT.

3.5 At all times, Harrow Hong Kong staff should conduct network communications with the utmost propriety, and avoid any Internet behaviour that may bring them or the School into disrepute.

3.6 Members of staff should not use social networking sites, or personal email accounts for communication with current pupils.

4. Content

4.1 Email correspondence should be treated in the same way as any other correspondence, such as a letter or a fax: as a permanent written record which may be read by persons other than the addressee and which could result in personal or the School's liability.

4.2 Members of staff and/or the School may be liable for the contents of an email message. No member of staff, therefore, should use someone else's account to send an email, unless in an emergency and it specifically states who that email is from. All ICT users should log off or lock their computers when not in use. Email is neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be presented in litigation. The audience of an inappropriate comment in an email may be unexpected and extremely widespread.

4.3 Members of staff should never use the School network, Internet or email for the following purposes:

- To abuse, vilify, defame, harass or discriminate (particularly, but not exclusively by virtue of sex, sexual orientation, marital status, race, colour, nationality, ethnic or national origin, religion, age, disability or Trade Union membership);
- To send or receive obscene or pornographic material;
- To injure the reputation of the School or in a manner that may cause embarrassment to the School as an employer;
- To spam or mass mail or to send or receive chain mail;
- To infringe the copyright or other intellectual property rights of another person;
- To perform any other unlawful or inappropriate act;
- To upload or publish externally images of School pupils or staff without permission; or
- To infringe the privacy of another person

4.4 Email content that may seem harmless to the sender may in fact be offensive to someone else. Members of staff should be aware, therefore, that in determining whether an email falls within any of the categories listed above, or is generally inappropriate, the School will consider the reaction and sensitivities of the recipient of an email.

4.5 If a member of staff receives inappropriate material by email, it should not be forwarded to anyone else. While it would be appropriate for members of staff to discourage the sender from sending further materials of that nature, it may also require it being reported to the Principal Deputy Head (Pastoral).

4.6 The School understands that members of staff cannot always control the messages that are sent to them. However, all members of staff must discourage third parties (such as family, friends or colleagues) from sending inappropriate messages to them. If a member of staff receives an inappropriate message or attachment to an email he or she must:

a. Send a message to the person who sent the inappropriate email which indicates that such messages should not be sent. An appropriate response looks like the following: "Please do not send me this type of material again. The contents of this email do not comply with the School's electronic communications policy. In sending me this email you are breaching the School's policies and putting me at risk of doing so. A breach of the School's electronic communications policy has serious consequences."

b. You may wish to forward a copy of this response (together with the inappropriate message) to the Principal Deputy Head (Pastoral) and/or the Director of ICT.

c. Delete the message.

4.7 Comments that are not appropriate in the workplace or the School's environment will also be inappropriate when sent by email. Email messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.

4.8 Members of staff should be aware that use of the School's ICT network in a manner inconsistent with this Policy or in any other inappropriate manner, including but not limited to use for the purposes referred to in paragraph 4.3 of this Policy, may give rise to disciplinary action, which may include termination of employment or contractor's engagement.

4.9 Internal email and other internal information should not be forwarded to destinations outside of the Harrow Hong Kong domain without the authority of the appropriate individual.

5. Data Protection and Privacy

5.1 In the course of carrying out duties on behalf of the School, members of staff may have access to, or handle personal information relating to others, including pupils, colleagues, contractors, residents, parents and suppliers. Email should not be used to disclose personal information of or about another except in accordance with the School's Data Protection Policy or with proper authorisation.

5.2 Data Protection legislation requires both members of staff and the School to take reasonable steps to protect any personal information held as a consequence of employment, from misuse and unauthorised access. Data Protection breaches may be treated as gross misconduct by the School, which could result in summary dismissal. Members of staff must, therefore:

- Take responsibility for the security of their School computer and any personal computers and removable storage devices (including mobile phones) that they may use as a consequence of their employment;
- Unless absolutely necessary, not use a personally owned home computer, laptop or any portable electronic device to store School confidential data (such as pupil/parent addresses, email addresses, telephone numbers, medical histories, staff information, etc.);
- Take all reasonable precautions if there is a need to transmit confidential data outside the School (either by email or the Internet, or by using removable storage media such as memory sticks, CDs, DVDs, removable hard drives, etc.), and to securely delete or destroy the data once it is no longer required;
- Contact the School's ICT department if they need any assistance or advice regarding appropriate security measures.

5.3 Members of staff are assigned a username and a password to use the School's electronic communications facilities, and must ensure that these details are not disclosed to anyone else and take steps to keep these details secure. It is, for example, strongly recommended that members of staff change their password regularly, and ensure that their username code and password are not kept in writing close to their working area.

5.4 Members of staff are expected to lock their screen or log-out when leaving their desk, and to log out and shutdown their computer overnight. This will avoid others gaining unauthorised access to the personal information of members of staff, the personal information of others and confidential information within the School.

5.5 In order to comply with the School's obligations under Data Protection legislation, members of staff are encouraged to use the blind copy option when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy.

5.6 In addition to the above, members of staff should be familiar with the School's Data Protection Policy and ensure that their use of email does not breach Data Protection legislation. The Compliance Manager should be contacted if there are any queries about compliance with Data Protection legislation.

5.7 The facility to automatically forward emails should not be used to forward messages to personal email accounts to ensure the integrity of the School's information and data. ICT may be able to provide solutions for accessing Harrow Hong Kong's email system when working away from the office or if remote access is required.

6. Distribution and Copyright

6.1 When distributing information over the School's computer network or to third parties outside the School, members of staff must ensure that they and the School have the right to do so, and that the intellectual property rights of any third party are not being violated.

6.2 Copyright law that may apply to any information that may need to be distributed must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through email without specific authorisation to do so. A similar caveat applies to the posting of the pupil photographs on the School's network.

6.3. If a member of staff is unsure about having sufficient authorisation to distribute the information, please contact the Marketing & Communications Manager in the first instance.

7. Confidentiality

7.1 As the Internet and email are insecure means of transmitting information, items of a confidential or sensitive nature should not be sent via email: there is always a trail somewhere and a copy saved, not necessarily only on the School's network server.

7.2 Members of staff must ensure that all emails that are sent from their School email address contain the School's standard disclaimer message. This message will be set to appear automatically on each outgoing email. Please contact a member of the ICT department if this feature is not working.

7.3 There is a risk of false attribution of email. Software is widely available by which email messages may be edited or 'doctored' to reflect an erroneous message or sender name. The recipient may, therefore, be unaware that he or she is communicating with an impostor. It is always important to maintain a reasonable degree of caution regarding the identity of the sender of incoming email and to verify the identity of the sender by other means if you have concerns.

7.4 Retention of messages takes large amounts of storage space on the network and can slow down performance. Members of staff should maintain as few messages as possible in their inboxes and outboxes, and delete old or unnecessary email messages regularly. If advised about exceeding the individual email storage limit, the ICT department should be contacted for assistance.

8. Social Media

8.1 The School recognises that many members of staff make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the School in these circumstances, members of staff must be aware that they can still cause damage to the School if they are recognised online as being one of its staff. Therefore, it is important that the School has strict social media rules in place to protect its position.

8.2 When logging on to and using social media websites and blogs at any time, including personal use on non-School ICT devices outside the workplace and outside normal working hours, members of staff must not:

- Conduct themselves in a way that is potentially detrimental to the School or brings the School or its pupils, contractors, residents, parents and suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content.
- Allow their interaction on these websites or blogs to damage working relationships with or between staff and pupils, colleagues, contractors, residents, parents and suppliers of the School, for example, by criticising or arguing with such persons.
- Include personal information or data about the School's staff, pupils, colleagues, contractors, residents, parents or suppliers without their express consent (an employee may still be liable even if staff, pupils, colleagues, contractors, residents, parents or suppliers are not expressly named in the websites or blogs as long as the School reasonably believes they are identifiable) - this could constitute a breach of Data Protection Act legislation, which is a criminal offence.
- Make any derogatory, offensive, discriminatory, untrue, negative, critical or defamatory comments about the School, its staff, pupils, contractors, residents, parents or suppliers (an employee may still be liable even if the School, its staff, pupils, contractors, residents, parents or suppliers are not expressly named in the websites or blogs as long as the School reasonably believes they are identifiable).
- Make any comments about any member of the School's staff that could constitute unlawful discrimination, harassment or cyber-bullying contrary to Equal Opportunities legislation or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying – members of staff can be personally liable for their actions under such legislation.
- Disclose any trade secrets or confidential, proprietary or sensitive information belonging to the School, its staff, pupils, colleagues, contractors, residents, parents or suppliers or any information which could be used by one or more of the School's competitors, for example information about the School's work, its products and services, technical developments, deals that it is doing or future business plans and staff morale.
- Breach copyright or any other proprietary interest belonging to the School, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work. If members of staff wish to post images, photographs or videos of their work colleagues or pupils, contractors, residents, parents or suppliers on their online profile, they should first obtain the other party's express permission to do so.
- Staff should not place on the internet, including social networking sites, any personal opinion or statement that might be construed as representing Harrow Hong Kong, that does not conform to the School's values and philosophy.

8.3 Members of staff must remove any offensive content immediately if they are asked to do so by the School.

8.4 Members of staff should remember that social media websites are public fora, even if they have set their account privacy settings at a restricted access or "friends only" level, and therefore they should not assume that their postings on any website will remain private.

8.5 Staff must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for example by placing their privacy settings at a high level and restricting the amount of personal information they give out, e.g. date and place of birth. This type of information may form the basis of security questions and/or passwords on other websites, such as online banking.

8.6 If a member of staff notices any inaccurate information about the School online, they should report this to the Head of Communications in the first instance.

9. Viruses

9.1 All external files and attachments will be automatically virus-checked using scanning software. The Internet is a potential host for computer viruses. The downloading of infected information from the Internet is potentially fatal to the School computer network. A document attached to an incoming email may have an embedded virus.

9.2 If a member of staff is concerned about an email attachment, or believes that it has not been automatically scanned for viruses, the ICT department should be contacted without opening the attachment or replying to the email.

10. Guidelines for staff on the use of internal emails

10.1 The School operates in a fast paced and, at times, highly pressured environment, in which email is accepted as one of the primary methods of communication used on a daily basis. Email may be the best way to communicate a particular message, but in an age of digital information 'overload', all staff should be mindful of the impact of an excessively email driven culture and make smart choices about what, when and how to communicate with others.

10.2 With many individuals now accessing emails across multiple personal and work devices, it is increasingly important to use email appropriately in a way that fosters productivity and efficiency whilst enabling staff to manage a reasonable work life balance.

10.3 Whilst it is the prerogative of the sender to send an email whenever they choose, it is also the recipient's prerogative to choose when to read their incoming emails, provided this is in line with the accepted levels of professional behaviour and aligned with the expectations of their role and responsibilities. There should be no general expectation that staff will read and respond to emails that are sent late at night, but it is expected that all emails will have some form of response within 24-48 hours of receipt (during term time) – even if this is simply a holding reply. If emails are received over the weekend, it may be necessary to respond quickly or send a holding reply, with a full response being sent on the next School day.

10.4 In terms of what is currently considered good practice:

- Professional salutations and sign-offs should always be used eg Dear … and then Best Wishes or Kind Regards. If an email trail between two people ensues, the salutation can be dropped.
- Think twice before using 'reply all', ensure the appropriate use of cc. and consider whether all participants of an email need to continue to be cc'ed or included in an email trail after the initial exchange.
- Think about the tone of the email and the way it may come across – remember that people from different cultures and backgrounds may interpret things differently. It is best, therefore, to avoid sarcasm, humour or colloquialisms, and to write as clearly as possible.
- Proofread every message and only add the email address once the email is finished and you have checked it. This will prevent any emails being sent accidentally and before they have been edited.
- If the content is sensitive, it is much better to have a meeting or talk on the telephone. However, if a sensitive email must be sent, you should read your message out loud before sending it, to ensure the tone is appropriate and to avoid misunderstandings.

- Automated ‘out of office’ notifications should be used when a member of staff is away from School or will be unavailable for an extended period of time.
- Nothing is confidential - so write accordingly and remain respectful, treating others with dignity, at all times.
- The School’s Social Vision: ‘a caring, respectful community in which everyone thrives’ is equally important in our online community.

11. General

11.1 The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's email and Internet facilities. Members of staff are encouraged to act with caution and take into account the underlying principles intended by this Policy.

11.2 This policy is subject to change and the current version is posted on the Staff Intranet (SharePoint).

Dinesh Alwani, Director of ICT
August 2024

Declaration

I recognise that, when online, a user's actions are logged by the servers and that any apparent breach of the law or School rules may be investigated. I accept that serious breaches of the rules for computer use will be dealt with as a disciplinary matter and, when applicable, police or local authorities may be involved.

The School reserves the right to charge, including any excess, for any loss or damage to computer equipment given into the keeping of any member of staff, that is not met by an insurance claim.

I understand the School's Social Vision statement: 'a caring respectful community in which everyone thrives', and agree to abide by this statement in all my online activity.

I have read and fully understand the above conditions and agree to observe them:

Signed

Print Name

Department

Date

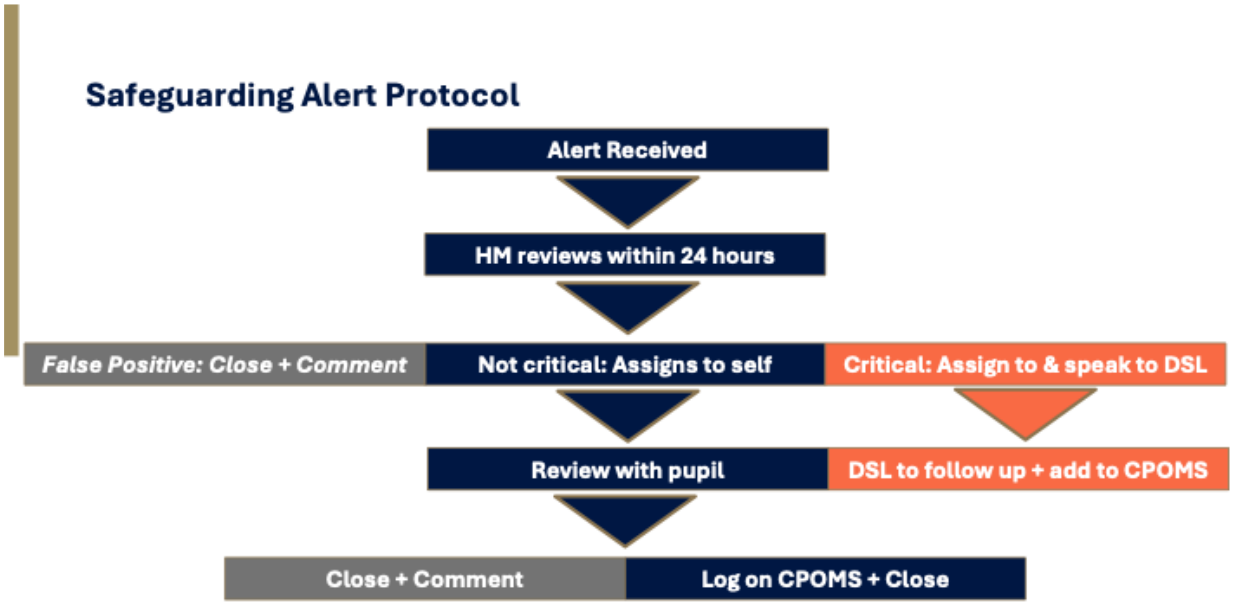
Please sign and return to the Director of Human Resources

E. A. Haydon
Head

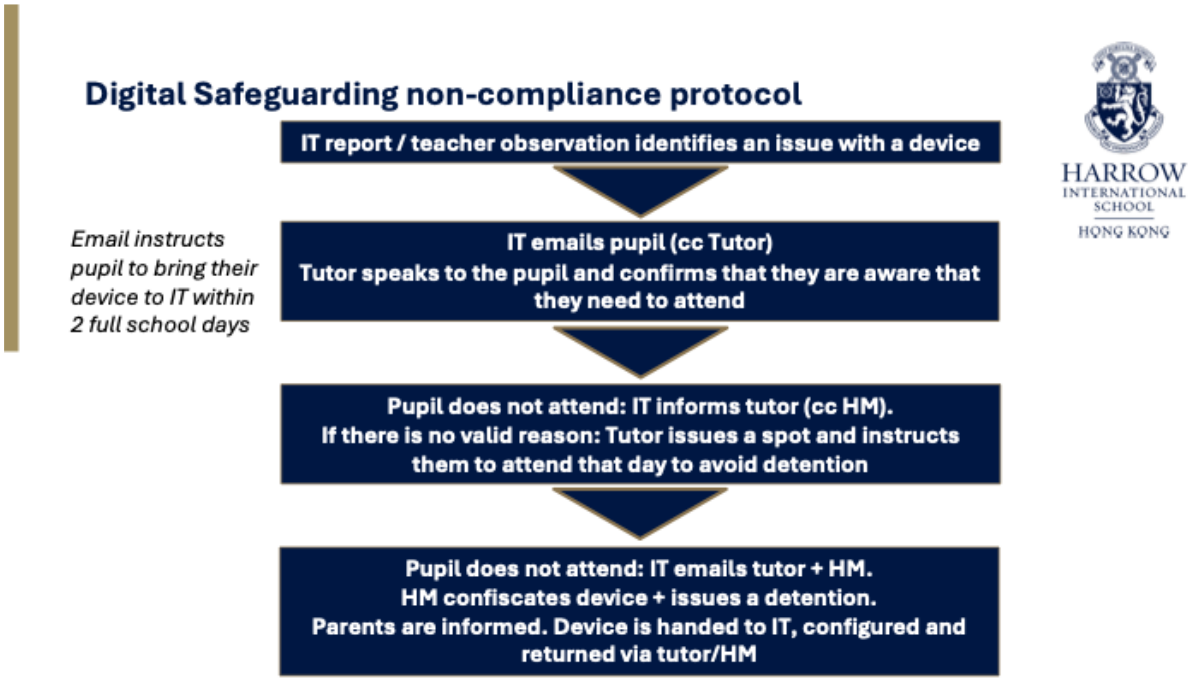
August 2024

Reviewed: 31 July 2024
Next review: 1 August 2025
Owner: Director of ICT

Appendix 3: Safeguarding Alert protocol



Appendix 4: Digital safeguarding non-compliance protocol



Appendix 5: Digital Safety Response Protocols

Purpose:

To outline steps to take when online safety concerns or incidents arise.

Response Steps:

1. **Reporting**:
    a. Pupils can report issues to teachers, the DSL, or other trusted adults.
    b. Parents/guardians can contact the school if they suspect an issue.
2. **Investigation**:
    a. The DSL will lead the investigation in collaboration with IT and relevant staff.
    b. All online incidents are documented for future reference.
3. **Actions**:
    a. Disciplinary actions based on severity, ranging from warnings to device restrictions.
    b. Support and counselling offered to pupils affected by cyberbullying or online abuse.
4. **Follow-up**:
    a. A follow-up with pupils and parents to ensure the resolution of the issue.

Alert Prioritisation for the pastoral response to filtering/monitoring issues:

Priority 1 - Immediate Response

- Self-harm/suicide related content
- Child protection/abuse material
- Immediate threats of violence
- Illegal content

Priority 2 - Same-Day Response

- Cyberbullying incidents
- Inappropriate content access
- Repeated attempts to bypass security

Priority 3 - 48-Hour Response

- Pattern of concerning behaviour
- Multiple attempts to access blocked content
- Unusual browsing patterns

Priority 4 - Weekly Review

- General policy violations
- Productivity concerns
- Non-educational use of resources

Appendix 6: Resources for Parents and Guardians

Purpose:

Provide parents with external tools and resources to help keep their children safe online.

Key Resources:

- **Online Safety Information:**
    - UK Safer Internet Centre: https://saferinternet.org.uk/
    - Common Sense Media: https://www.commonsensemedia.org/
    - Internet Matters: https://www.internetmatters.org/
    - Parent Info: https://www.educateagainsthate.com/resources/parent-info/
- **Cyberbullying Prevention:**
    - StopBullying.gov: https://www.stopbullying.gov/
    - ChildNet International: https://www.childnet.com/
    - Ditch the Label: https://anti-bullyingalliance.org.uk/aba-our-work/our-members/core-members/ditch-label
    - The Cybersmile Foundation: https://www.cybersmile.org/
- **Parental Controls and Monitoring:**
    - National Online Safety Guides: https://nationalcollege.com/guides/what-parents-need-to-know-about-online-content-10-tips-to-keep-your-children-safe-online
    - OpenDNS: https://support.opendns.com/hc/en-us/articles/227988127-Getting-started-About-using-OpenDNS
    - Qustodio: https://www.qustodio.com/en/
    - Screen Time: https://support.apple.com/en-us/108806

Appendix 7: Glossary of Terms

Purpose:

Define technical and safeguarding terms used in the policy.

Key Terms:

1. **Pupil Safety:** The safety and well-being of pupils.
2. **Digital Citizenship:** The responsible use of technology by pupils to engage positively and safely in the digital world.
3. **Positive Digital Culture:** A culture that fosters respect, inclusion, and responsible online behaviour.
4. **Digital Risks:** Online dangers such as cyberbullying, privacy breaches, and online harassment.
5. **Incident Reporting:** Procedures for reporting and responding to online safety incidents.
6. **Safeguarding Measures:** Technological, educational, and policy-based measures to protect pupils from online risks.
7. **Online Learning Platforms:** Platforms used for online learning activities.
8. **Personal Devices:** Laptops, tablets, and other devices used by pupils and staff.
9. **School-Issued Devices:** Devices provided by the school for educational purposes.

Appendix 8: LightSpeed Filtering and Automated Alerts Schedule

Lower School pupils

Period	Schedule	Filter	Monitor	Alert
In School rules	7:00 AM - 4:30 PM	On (LS Filter)	On	On
Out of School rules	4:30 PM - 6:59 AM and Non-school days	On (LS filter)	Off	Off

Prep School Day pupils

Period	Schedule	Filter	Monitor	Alert
In School rules	7:00 AM - 4:30 PM	On (PS Filter)	On	On
Out of School rules	4:30 PM - 6:59 AM and Non-school days	On (OOS filter)	Off	Off

Prep School Boarders

Period	Schedule	Filter	Monitor	Alert
In School rules	7:00 AM - 4:30 PM	On (PS Filter)	On	On
	4:30PM – 6:59AM	On (OOS filter)	On	Off
Out of School rules	Non-school days	On (OOS filter)	Off	Off

Year 9 Day pupils

Period	Schedule	Filter	Monitor	Alert
In School rules	7:00 AM - 4:30 PM	On (Y9 Filter)	On	On
Out of School rules	4:30 PM - 6:59 AM and Non-school days	On (OOS filter)	Off	Off

Year 9 Boarders

Period	Schedule	Filter	Monitor	Alert
In School rules	7:00 AM - 4:30 PM	On (Y9 Filter)	On	On
	4:30PM – 6:59AM	On (OOS filter)	On	Off
Out of School rules	Non-school days	On (OOS filter)	Off	Off

Senior School Day pupils

Period	Schedule	Filter	Monitor	Alert
In School rules	7:00 AM - 4:30 PM	On (SS Filter)	On	On
Out of School rules	4:30 PM - 6:59 AM and Non-school days	On (OOS filter)	Off	Off

Senior School Boarders

Period	Schedule	Filter	Monitor	Alert
In School rules	7:00 AM - 4:30 PM	On (SS Filter)	On	On
	4:30PM – 6:59AM	On (OOS filter)	On	Off
Out of School rules	Non-school days	On (OOS filter)	Off	Off

Appendix 9: Data Safeguarding and Retention of pupil monitoring data

1. **Data Transmission**

- Weekly reports are sent as SharePoint links within emails, therefore there is no data transmission risk

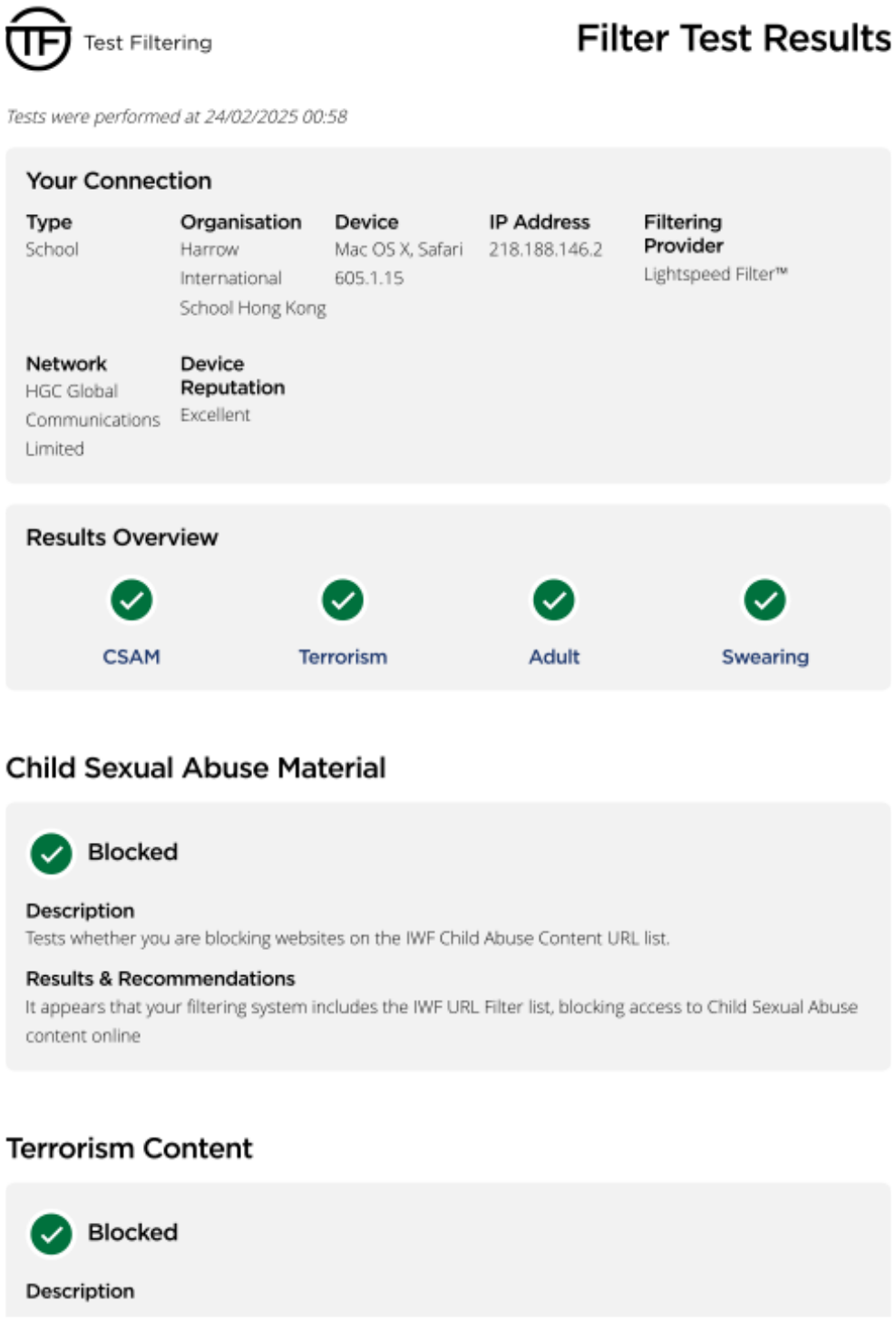
2. **Data Storage**

- Location: SharePoint [House Pastoral Team Reports/Documents/Firewall Reports]
- Format: Encrypted database with access controls to specific individuals
- Backup: SharePoint data is automatically backed up through M365

3. **Data Retention Periods**

- Web activity logs: 90 days
- Screen captures: 30 days
- Real-time monitoring data: 60 days
- Alert records: 90 days
- Firewall reports: 90 days

Appendix 10: Test Filtering Results



Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

Results & Recommendations
It appears that your filtering system includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

Adult Content

Blocked

Description
Test whether your Internet filter blocks access to pornography websites

Results & Recommendations
It appears that your filtering system includes blocking for adult content. This indicates that your system has a list of adult websites or pages that are actively being blocked.

The test only checks to see if blocking is in place, and does not measure the effectiveness of the blocking across the range of available sources. Check with your filter provider that your system is setup in the most effective way, and matches your policy and needs.

Offensive Language

Blocked

Description
Accesses a page containing offensive language to test if your filtering software blocks it

Results & Recommendations
It appears that your filtering system includes blocking for offensive language

Educational Excellence *for* Life and Leadership

數位保障政政策

HARROW INTERNATIONAL SCHOOL HONG KONG

1. 介绍

哈羅香港國際學校致力於為所有學生提供一個安全可靠的學習環境，無論是在實體課堂還是在數字世界中。本數位保護政策旨在為學校社區的所有成員創造一個安全可靠的數位環境，並促進負責任的數位公民意識。

2. 關鍵原則

- **學生安全**：學生的安全和福祉是我們的首要任務。
- **正向數位文化**：我們提倡積極和負責任的數位文化，促進尊重和包容，符合學院的價值觀和社會願景。
- **數位素養教育**：我們對學生進行網路風險、網路霸凌、隱私和負責任的線上行為的教育。
- **事件報告**：我們有明確的報告和回應線上事件的程序。
- **協作**：我們與家長和監護人合作，確保線上安全。

我們方法的關鍵原則在數字保護政策資訊圖表概述。

3. 保障措施

為確保安全可靠的數位學習環境，哈羅香港國際學校實施了一套全面的保障措施。這些措施包括數位素養教育計畫、技術解決方案和政策，以保護學生免受網路風險並促進負責任的數位公民。

3.1 技術（行動裝置政策）

- **Apple Classroom：** Apple Classroom 提供監控課堂活動摘要的平台，使教師能夠保持學生參與度的概覽，並透過所謂的實體監控來支援線上安全。此外，它能夠即時監控學生活動，使教師能夠快速識別和解決任何不當或有風險的線上行為，從而有助於保護學生，確保學生在課堂上的數位學習體驗中保持專注和安全。

- **LightSpeed 保護軟體**：該工具整合了內容過濾、監控和機器學習掃描，透過有效監控和管理線上活動來創建安全的數位環境。它在防止危險的線上行為方面發揮著至關重要的作用，並確保用戶只能存取安全且經過批准的線上資源，從而降低暴露於可能危及資料安全的惡意網站或網路釣魚嘗試的風險。LightSpeed 安裝在所有註冊學生擁有的 MacBook（高中）和 iPad（預科班和預科學校）以及學校擁有的設備上。這種全面的覆蓋範圍確保了所有平台上一致的保護和監控。

- **LightSpeed 過濾器：** LightSpeed 過濾器會阻止不適合學生使用的網站和應用程序。這包括通過應用程序、VPN 和網絡共享到 4G/5G 熱點的流量。

- **LightSpeed 監視器：** LightSpeed 監視器提供有關學生線上活動的全面報告，包括在嘗試存取已被封鎖的網站時進行記錄。

- **LightSpeed 警報**：LightSpeed Alert 掃描在線內容以查找自殘、網絡欺凌或暴力的警告信號，這些信號會轉發給輔導領袖和學校的 DSL，以便及時干預。通過這種方式，它在風險最高的情況下提供主動監控。

- **裝置 MAC 位址過濾**：只有經註冊學校的 MDM，Jamf Pro 的裝置才能透過學校的 WiFi 網路存取網路。以這種方式按設備過濾可確保只有配備所需軟體的經批准的設備才能存取學校的 Wi-Fi。這項措施是為了支持合規性，特別是在更換學生設備的情況下。

- **防火牆**：學校實施強大的防火牆系統，主動監控和阻止對不適當、惡意或非教育網站的訪問。這包括與遊戲、社交媒體、成人內容、代理伺服器和其他潛在有害材料相關的內容。該系統會產生全面的報告，詳細說明嘗試存取被封鎖的網站，並由 ICT 部門和 DSL 進行審查。ICT 部門審查匿名和匯總數據，以識別模式並根據需要調整過濾策略，DSL 審查與個別學生相關的問題。這種積極主動的方法可確保學生保持對教育內容的關注，同時保護他們免受線上威脅。防火牆的智慧分類系統會定期自動更新，以應對新的線上威脅並保持與學校教育目標的一致性。

- **透過學校的 MDM，Jamf Pro 停用管理員存取學生擁有的裝置：**為了防止學生安裝遊戲或其他分散注意力的應用程式，所有 3 至 9 級的 MacBook 和 iPad 上都會停用管理員存取權限。此外，Apple Store 隱藏在 iPad 上。家長可以選擇在孩子的裝置上設定「家人共享」帳戶。透過此設置，他們可以管理裝置上安裝的應用程式和程序，同時確保其符合學校的學習目標。

- **定期審核**：學校定期（至少每年）對技術工具進行審核，以確保它們保持有效和最新。

- **數據隱私合規性**：學校通過定期審查數據處理程序，確保遵守當地的數據保護法規。

- **設備預期使用情況和軟體簽入報告：** IT 監控設備的使用情況，以確保遵守保護軟體的安裝和維護。例如，如果學生設法卸載 Jamf，它將向 IT 部門產生警報。這些報告和警報在輔導團隊的支持下引發調查。詳情請參閱附錄 4，數碼保障違規協議。

3.2. 寄宿公寓的定時 Wi-Fi 接入

為了促進健康的上網習慣、鼓勵集中學習並確保充足的休息，寄宿公寓的 Wi-Fi 接入遵循時間表。具體來說，WiFi 接入會在夜間關閉。這項措施有助於平衡數位參與與線下活動，並促進健康的睡眠時間表。

- **初中宿舍（6-8 年級）：** Wi-Fi 在晚上 8：30 至早上 7：30 關閉。
- **高中宿舍（9-11 年級）：** 晚上 10：30 至早上 6：30 關閉 Wi-Fi。
- **預科宿舍（12-13 年級）：** Wi-Fi 在晚上 11：00 至早上 6：00 關閉。

較晚的截止時間可以滿足年齡較大的學生的學業需求，並允許稍微延長晚上的個人活動時間。

3.3 過濾和監控

在哈羅香港，我們使用過濾軟體來限制對不當內容的訪問，並監控學生設備上的線上活動，以確保負責任和安全的使用。學生 ICT 行為準則定義了預期的在線行為，所有學生和家長/監護人在訪問學校網絡之前都必須同意它。

監控有兩種形式：通過 LightSpeed 過濾器和網絡防火牆記錄嘗試訪問過濾站點，以及通過 LightSpeed 主動監控危害警告指標。

更新過濾規則：如果網站被錯誤封鎖，學生和教職員都可以向學校的 ICT 部門報告。他們可以選擇向 askit@harrowschool.hk 發送電子郵件 或填寫 Microsoft 表格：點擊這裡。這確保了快速解決存取問題，保持對線上資源的順利、不間斷的存取。

監控系統的任何變更都會經過審批流程並記錄下來，從而實現審計跟踪，確保透明度，並且個人無法進行單方面更改。

為確保我們的篩選規則適當，我們會定期審查和更新這些規則。英國更安全的互聯網中心獲得認可 測試過濾公用程式 至少每年用於審查學校的過濾規則。
見附錄 8。

3.4 線上活動的報告和監控

哈羅香港加強了線上活動的報告和監控協議。這些協議確保通過防火牆和 LightSpeed 系統收集的數據得到有效和負責任的審查和使用，以維護學生的安全和福祉，同時遵守《個人資料（隱私）條例》（PDPO）。

3.4.1 防火牆報告和輔導團隊的審查

學校的防火牆系統會產生有關嘗試存取被封鎖網站和其他受限制線上活動的詳細報告。這些報告由輔導團隊根據以下準則進行審查：

a. 資料範圍：
- 報告將盡可能包含匿名或匯總數據，重點關注不當存取嘗試的模式。
- 對於已識別的事件，可能會存取特定使用者資料（例如裝置識別碼、時間戳記和 URL）來調查違反學生 ICT 行為準則的行為。

b. 存取控制：
- 防火牆報告通過安全訪問鏈接發送，只有輔導團隊的授權成員才能訪問。

c. 目的：
- 識別不當線上行為的趨勢，並相應地調整政策和教育。
- 解決學生試圖存取有害或不當內容的個別事件。

d. 頻率：

- 資訊及通訊科技部門每週向輔導團隊提供防火牆活動摘要。
- 重大事件（例如，嘗試存取成人內容或惡意網站）的即時警報將立即升級。

3.4.2 LightSpeed 輔導團隊的報告和審查

LightSpeed 提供先進的監控功能，包括針對自殘、網路霸凌或暴力等危險線上行為的警報。下列通訊協定會控管此資料的使用：

a. 資料範圍：

- LightSpeed 根據預先定義的風險指標產生警報，包括標記的關鍵字、異常瀏覽活動、螢幕擷取報告和監控活動日誌。
- 開啟監控後，系統會收集 Web 活動數據，包括 URL 存取記錄、瀏覽持續時間、網站類別、下載活動、搜尋查詢、頻寬使用情況、帶時間戳記的 Web 會話和瀏覽器資訊。
- 所有警報和報告都包含基本標識符，例如設備信息、用戶配置文件、時間戳記和標記內容，以及屏幕監控數據，包括屏幕截圖捕獲、活動時間表和應用程序使用日誌。

為遵守香港《個人資料（私隱）條例》（《私隱條例》），系統遵守特定的資料保留期限：網絡活動日誌保存 90 天，截圖保存 30 天，實時監控數據保存 60 天，警報記錄保存 90 天。

b. 輔導領袖的監督責任：

- 存取嘗試分析 – 審查存取被封鎖資料的頻繁嘗試，監控試圖規避過濾系統的模式，並追蹤對特定類別關注的重複存取嘗試。
- 高風險內容監控 - 審查訪問有害或危險材料的嘗試，監控與自殘、暴力或極端主義相關的搜索，並跟踪對不適合年齡的內容的訪問嘗試。
- 行為模式分析 - 審查搜索和瀏覽模式所花費的時間，監控在線活動的異常時間，並跟踪可能表明問題的典型使用模式的變化。
- 政策合規性 - 確保遵守可接受的使用政策、監控學校設備政策的合規性並跟踪教育資源的適當使用

審查和回應頻率：

- LightSpeed 門戶網站向輔導團隊（年級領導、社監 和 DSL）提供 LightSpeed 警報的摘要。
- 關鍵警報會在檢測到後一小時內自動發送給 DSL 和輔導領袖。
- 高優先順序警示必須每天審查，並在當天收到回應。
- 有關更多詳細信息，請參閱附錄 3。
- 標準過濾器報告將每週審查一次。
- 應定期進行趨勢分析。

d. 存取控制：

- 對 LightSpeed 報告的訪問僅限於輔導團隊。
- 針對保護問題的警報會直接發送給指定保障負責人 （DSL） 以立即關注。

- 對 LightSpeed 資料的所有存取都是透過受限權限、密碼保護和記錄的，並定期進行審核以確保遵守存取策略。

e.目的：

- 及時採取干預措施以保護問題，例如識別有受到傷害風險的學生。
- 通過解決不當的在線行為來支持學校的行為政策。
- 透過確保專注且安全的數位學習環境來提高教育成果。

3.5 存取資料和角色

根據《個人資料（PDPO）》和資料最小化和目的限制的原則，對防火牆和 LightSpeed 資料的存取受到基於角色的權限的嚴格管理：

1. 具有存取權限的角色：

- ICT 輔導聯絡： 負責管理和維護防火牆和 LightSpeed 系統並生成報告。ICT 輔導聯絡員無法訪問學生數據，但有助於為輔導團隊生成和傳播報告。
- 學生的輔導領袖（高年級的宿生家長和低年級的年級領導）：有權審查與學生保護和行為管理相關的報告和警報。
- 指定保護負責人 （DSL） 負責：
    - 監控和審查 LightSpeed 在所有年級組中生成的自動保護警報
    - 管理任何標記的保護問題的調查過程
    - 高級領導團隊 （SLT）： 可以訪問匯總和匿名數據，以進行戰略決策和政策更新。

2. 數據類別：

- 匯總數據：用於趨勢分析和政策調整（例如，識別被阻止的網站訪問模式）。
- 可識別資料：僅在調查特定事件、行為或保護問題時存取。

3. 存取協定：

- 所有對數據的訪問都會被記錄下來並接受定期審計。
- 有權存取的員工必須完成有關資料保護和保護協議的年度培訓。
- 未經授權的訪問或濫用數據將根據學校的政策受到紀律處分。

3.6 資料的使用

透過防火牆和 LightSpeed 系統收集的資料僅用於以下目的，符合《個人資料（私隱）條例》：

5. 保護學生：
    a. 偵測並應對網路霸凌、自殘或接觸有害內容等風險。
    b. 支持 DSL 和輔導團隊提供及時的干預。
6. 行為管理：
    a. 監控學生 ICT 行為準則的遵守情況。
    b. 通過學校的行為政策解決不當的在線行為。
7. 政策制定：
    a. 識別線上活動的趨勢，為數位保護政策和過濾規則的更新提供資訊。

b. 根據新出現的風險加強學校的數位素養課程。

8. 教育支持：
    a. 確保學生在數位學習活動期間專注於教育內容。
    b. 促進積極、安全的數位學習環境。

3.7 遵守香港《私隱條例》

香港哈羅國際學校通過遵守以下原則，確保所有數據收集、存儲和處理活動都符合《私隱條例》：

6. **資料最小化**：僅收集保護、行為管理和教育目的所需的資料。
7. **目的限制**：資料僅用於本政策中概述的目的，不會與未經授權的各方共享。
8. **透明度**：學生、家長和教職員了解透過防火牆和 LightSpeed 系統收集的資料及其預期用途。
9. **安全性**：資料安全存儲，存取僅限授權人員，並受到強大的技術保護措施的保護。
10. **保留：**資料僅在實現其預期目的所需的時間內保留，此後將安全刪除。

3.8. 數字素養教育

哈羅香港確保我們所有學生的教育都包括保持上網安全並保障他們福祉所需的數字知識和技能。這是**數字素養**課程的一個組成部分，通過低年級的計算機課程以及高年級的計算機科學課程和 PSHE 課程的組合進行教授。所教授的組成部分符合英國政府的「互聯世界教育」框架，並在數位策略政策中進行了詳細說明。學生數位安全指南包括具體提及「4C」帶來的線上威脅：內容、聯繫、行為和商業。

家長網絡研討會：學校每年為家長提供網絡研討會，幫助他們了解一些必要的數字素養技能以及他們可以在家中做些什麼來支持他們的孩子。

3.9 保護和人工智慧

生成式 AI 工具對學生的福祉構成特定且重大的保護風險，包括但不限於接觸有害內容，包括 AI 生成的兒童性虐待材料 （AI-CSAM）、霸凌、誘騙和騷擾。此外，濫用個人資料可能會導致隱私外洩、產生虛假或誤導性資訊，並增加網路攻擊、詐欺和詐騙的風險。未經授權使用受版權保護的資料可能會導致智慧財產權問題，人工智慧系統中現有偏見的延續或放大可能會導致不公平待遇或歧視。

我們致力於確保安全和負責任地使用人工智慧技術，我們的措施在我們的人工智慧政策中進行了概述。這些包括：

- **人工智慧素養教學** 作為數位素養課程的一部分
- **默認情況下，生成式 AI 工具作為**預備學校和預備學校中 LightSpeed 過濾規則的一部分被阻止
- **所有生成式 AI 應用程式**在解鎖和/或在課堂上使用之前都會經過徹底的風險評估，以評估其益處和潛在風險，確保遵守資料保護、兒童安全和智慧財產權法等法律責任。

3.10 手機和不受限制的互聯網訪問

移動電話提供離散、不安全和不受監控的互聯網訪問，因此降低風險是本政策的一個特別考慮因素。使用移動或個人便攜式 5G 路由器將移動設備（iPad 或 MacBook）連接到互聯網而無需通過我們的網絡過濾器的能力增加了這種風險。本政策透過多種方式解決此問題：

- **上課時間手機使用限制：** 嚴格限制在校園內攜帶和使用手機。
- **旅行期間使用手機的限制：** 低年級和預科學校的學生不應使用手機，除非獲得特別許可，這包括 SCA 和固定裝置等場外活動。高年級學生可以在旅途中和正式休息期間使用設備。過夜旅行應遵守以下登機手機使用政策，或者如果旅行性質需要保持無手機環境。更多詳細資訊請參閱旅行和參觀政策。
- **使用網絡共享的限制：**以確保在校期間的在線活動受到保護。禁止與手機或便攜式 5G 路由器進行網絡共享，這包含在學生每年簽署的《學生 ICT 行為準則》中。
- **LightSpeed 代理繼續保護移動寬帶**：作為設備上安裝的軟件，對於 MacBook（高中）和受監督的 iPad（Pre-Prep 和 Prep School），LightSpeed 即使在網絡共享到手機時也會繼續過濾和監控互聯網活動。
- **透過 Jamf MDM 進行抽查**：IT 部門每天至少在連接到非學校網路的受管理裝置上產生 3 次自動報告。輔導團隊使用這些信息來解決不合規問題。
- **晚上寄宿生手機使用和繫留限制：**晚上寄宿生使用手機受到管理。9 年級和 10 年級的高年級寄宿生在晚餐和準備時間下午 6.30 至晚上 8.30 交出手機。他們可以在晚上 8 點 30 分領取手機聯繫家長，直到晚上 8 點 45 分。 所有手機和設備均在晚上 8 點 45 分至早上 7 點 45 分之前在 9 年級和 10 年級之前上交。 對於 11 年級，電話和設備在晚上 9.30 至次日早上 7.45 之間通宵上交。在下午 5.30 至 6 點之間，初中部學生可以使用手機。 寄宿生可以在每天晚上 7.30 至晚上 7.45 之間使用 6 年級和 7 年級的電話給家長打電話。8 年級寄宿生可以在晚上 8.15 至晚上 8.30 之間使用手機。 所有電話和設備都經過夜間保護，直到第二天早上 7.30 這得到了家庭輔導團隊的物理監控和 IT 網絡共享報告的支持。

4. 事件報告和回應

4.1 防火牆和 LightSpeed 報告

防火牆和 LightSpeed 系統產生的報告將整合到學校的事件回應流程中，如下所示：

報告：

3. 來自 LightSpeed 的關鍵警報（例如，自殘指標）會立即上報到 DSL。
4. 涉及反覆嘗試存取受限制內容的防火牆事件將被標記為輔導團隊進行調查。

4.2 學生報告

- **報告**：鼓勵學生向值得信賴的成年人報告網路安全問題，例如教師、HM 或指定保護負責人（DSL）。
- **匿名報告**：學校提供了一個安全的在線表格，可通過學校內聯網訪問，用於匿名報告數字安全問題，該表格直接路由到 DSL。

4.3 數位安全回應協議

學校通過其行為政策處理在線事件，其中包括調查程序、紀律措施以及對相關學生的支持。

- DSL 與 ICT 部門和相關工作人員合作領導調查。
- 紀律措施和支援計劃是根據學校的行為和保障政策實施的。

4.4 回應及時性

學校對所有報告的事件保持嚴格的響應時間表，並按嚴重程度分類。重大事件（危及生命）需要立即關注，必須在報告後一小時內解決，而其他問題則在 48 小時內迅速處理，以確保對所有案件給予適當關注。在整個事件管理過程中，相關利害關係人會定期收到有關報告問題的進度和解決方案的狀態更新。資訊及通訊科技部門和高級管理層每月都會審查這些回應協議的有效性，以維持和改進服務標準，確保以最佳方式處理所有安保和安全問題。

4.5 說明文件

所有事件均會記錄在案，並保留數據日誌以作審計之用，以符合《私隱條例》的規定。

5. 員工職責

- **培訓**：所有員工都接受有關數位保護程序及其在促進安全線上環境方面的作用的培訓。
- **監控和報告**：輔導團隊監控學生的在線活動，並向 DSL/DDSL 報告任何問題。
- **負責任的行為建模**：員工按照員工 IT 可接受使用政策（每年閱讀並簽署）塑造負責任的數位行為。
- **與家長溝通**：輔導團隊定期與家長溝通網路安全，並就如何應對家庭數位風險提供指導。

6. 父母的責任

- **溝通**：鼓勵家長定期與孩子討論網路安全，並對負責任的線上行為建立明確的期望。
- **監控**：鼓勵家長監控孩子的線上活動並確保安全的網路使用。
- **協作**：敦促家長表達對孩子線上安全的擔憂，並與學校合作解決這些問題。
- **資源**：學校為家長提供資源，讓他們隨時了解網路安全問題，包括信譽良好的網路安全網站和工具的連結。

7. 審查和更新

哈羅香港致力於確保這項政策保持有效、相關，並與技術進步、新興的網路威脅和不斷變化的保障需求保持一致。審查過程旨在透過學校社區的協作和回饋來促進持續改進。

7.1 定期檢討及諮詢

- **年度審查**：本政策將進行年度審查，以確保其符合最新的保護措施、技術發展以及遵守香港個人資料（私隱）條例（PDPO）。

- **利害關係人諮詢**：
  - 將積極尋求包括教職員、學生、家長和州長在內的主要利益相關者的反饋，以確保該政策反映學校社區的多樣化需求。
  - 諮詢過程可能包括調查、研討會、焦點小組和非正式討論，以收集有價值的見解和建議。
- **事件數據分析**：將分析來自防火牆和 LightSpeed 報告系統的數據以及事件日誌，以識別趨勢、評估當前措施的有效性並解決任何反覆出現的問題。

7.2 報告協議的有效性

- 防火牆和 LightSpeed 報告協議的有效性將在年度政策評估期間進行專門審查。
- ICT 部門、輔導團隊和指定保護負責人 （DSL） 的反饋將用於評估和提高監控、報告和響應流程的效率。
- 將及時實施改進建議，以維持健全的保護框架。

7.3 政策可訪問性

- 學校網站上提供了關鍵保護措施的摘要，包括報告協議和數位素養指南，以確保清晰度和理解。

7.4 持續回饋機制

- 反饋機制允許利益相關者就政策提供持續的意見。
- DSL 和 ICT 部門將定期審查反饋，以確保及時更新和改進。
- 我們的數位保護政策透過結構化的回饋管道保持有效性，使利害關係人能夠參與並及時改進。

7.5 社群參與

- 為家長舉辦的學期 PGCG 會議和學院代表會議，以及家長網路研討會和資訊晚會
- 學生會會議、學生數位級長和社制數位代表
- 通過導師時間和學生數字級長的學生聲音
- 部門會議上的員工諮詢

7.6 動態更新

- 政策將根據需要進行更新，以解決以下問題：
- 新的線上風險或保障挑戰。
- 當地法規的變化，例如《私隱條例》的更新。
- 技術進步或採用新的保護工具。
- 如有需要，將透過官方管道（包括電子郵件通知和學校網站）及時向利害關係人傳達中期更新。

7.7 透明度和問責制

- 該政策的所有更新都將被記錄下來，並向利益相關者提供更改摘要以提高透明度。
- 高級領導團隊 （SLT） 將監督審查過程，以確保問責制並與學校的保護目標保持一致。

7.8 在幼兒中心使用流動電話

不得在幼兒中心內任何地方有兒童在場的情況下使用手機（緊急情況除外）。
只能使用學校擁有的數碼設備拍攝學生及其學習的照片和/或視頻。

8. 附錄

- **附錄一**：學生資訊及通訊科技行為守則
- **附錄 2**：員工 ICT 可接受使用協議
- **附錄三**：保障警示協議
- **附錄 4**：數位保護不合規協議
- **附錄 5**：數位安全回應協議
- **附錄 6**：家長和監護人的資源（例如，網路安全網站的連結）
- **附錄 7**：術語表
- **附錄 8**：Lightspeed 配置設置
- **附錄 9**：資料保護和保留
- **附錄 10**：測試過濾結果

評論日期：2025 年 9 月
下一篇評論：2026 年 8 月
擁有人： 助理校長（數碼策略、評估及追蹤）
版本：2

附錄 1：學生資訊及通訊科技操守守則（2024/25）[高年級]

鏈結在這裡： 學生 ICT 行為準則 2025-26

HARROW INTERNATIONAL SCHOOL HONG KONG

2025-26 年低年級學生數位行為準則

學校有責任確保香港哈羅國際學校的每位學生安全、負責任地使用數碼設備、互聯網和通訊設備。在使用設備之前，所有學生都必須閱讀、理解並簽署本行為準則。這適用於使用任何連接到學校網絡的設備，包括 iPad、MacBook 和其他數字設備。

1. 學生不得使用他人帳戶或讓自己的帳戶被他人使用。
2. 除非老師指示，否則學生不應通過互聯網或任何其他方式相互發送信息。
3. 未經許可，學生不得分享有關學校或學校中任何個人的任何個人信息，例如文字或圖像。
4. 學生不應嘗試訪問、發送或存儲任何不適當的信息，包括圖像。
5. 使用設備（包括 iPad）時，所有學生都必須遵守 iPad 黃金法則，如下所示和在教室中。

如果未履行上述協議之一，教師有權限制學生使用其設備。

我已閱讀並理解小學部數碼行為準則，並同意始終遵守這一點。

學生簽名：_____

日期：_____

附錄二： 員工資訊及通訊科技可接受使用協議 （2024/25）

本文件規定了香港哈羅國際學校的所有教職員在使用任何設備進行電子通訊或使用學校的資訊通信技術設施時應遵守的安全、管理和內部規則。所有教職員均應密切留意本政策的條款，以盡量減少因濫用電郵或互聯網設施而可能對自己、學生及學校造成的潛在困難。本政策適用於本校所有員工、員工的常住家庭成員或任何其他使用學校資訊及通訊科技設施的客人。

學校網絡可供整個學校社區使用，包括學術和教育支援人員、學生、家長和訪客，學校有責任確保哈羅香港的每位用戶負責任地使用電腦設備和互聯網，以及手機和其他通訊設備。用戶應期望他們在學校網絡上的電腦使用受到監控，儘管這將是相稱的，即僅在必要的情況下，並且以限制對隱私的潛在侵犯的方式進行。所有用戶都應在支持學校願景聲明、目標和目標的活動中使用學校的 ICT 系統、資源和相關應用程序。因此，資訊及通訊科技資源不得用於任何非法或不道德的目的，並應盡量減少娛樂或個人用途。同樣，用戶不應從事任何可能破壞網絡有效運行的活動。

1. 學校財產

1.1 學院認可並歡迎教職員在製作和儲存教材方面的創造力，以支援教學、學習和管理。值得注意的是，根據法律條文，員工、承包商和居民在履行正常職責時在學校網路上創建和儲存的文件和電子郵件在技術上仍然是學校的財產。如對版權及知識產權有任何疑問，我們鼓勵員工徵詢處長的意見。

1.2 根據本政策中概述的進一步規定，教職員、承包商和居民在學校網路上建立和儲存的供其私人和個人使用的文件和電子郵件仍然是創建者的財產。

2. 監控

2.1 本校的電腦網絡是一種商業和教育工具，主要用於商業或教育目的。因此，員工有責任以適當、專業和合法的方式使用這些資源。

2.2 學校系統上的所有訊息和文件都將被視為與教育或業務相關的訊息和文件，並可能受到監控。因此，教職員不應期望在學校電腦網絡上傳輸或儲存的任何資訊或文件是完全私密的。

2.3 教職員亦應注意，學院設有自動監察及過濾網際網使用情況的系統，包括教職員瀏覽的網站和內容，以及他們使用網際網路的時間長短。

2.4 教職員應認識到，如果擔心可能被濫用，學校可能需要檢查其內容，從而在編寫電子郵件時認識到。

2.5 電子郵件將由學校在認為適當並符合法定要求的情況下存檔。

3. 個人使用

3.1 教職員可透過學校網絡使用互聯網及電郵設施收發個人資料，但須盡量減少使用，且不得妨礙其執行工作。

3.2 但是，出於個人目的使用學校網絡仍受本政策中其他描述的相同條款和條件的約束，無論它是標記為私人還是機密。

3.3 在共享資訊科技設施的情況下，員工應尊重同事的需求，並及時有效地使用電腦資源。

3.4 在工作時間內出於個人原因過度或不當使用電子郵件或互聯網設施可能會導致紀律處分。例如，未經資訊及 ICT 總監同意，教職員不得下載大型視訊/音訊檔案供個人使用，亦不得下載大量影像，亦不得下載或安裝電腦程式。

3.5 在任何時候，哈羅香港員工都應以最適當的方式進行網絡通信，避免任何可能損害他們或學院聲譽的互聯網行為。

3.6 教職員不應使用社交網站或個人電郵帳戶與在校學生溝通。

4. 內容

4.1 電子郵件通信應與任何其他通信（例如信件或傳真）相同：作為永久書面記錄，收件人以外的人可以閱讀，並可能導致個人或學校承擔責任。

4.2 教職員及/或本校可能須對電郵內容負責。因此，任何員工都不應使用他人的帳戶發送電子郵件，除非在緊急情況下，並且明確說明該電子郵件來自誰。所有資訊及通訊科技使用者在不使用電腦時，應登出或鎖定電腦。電子郵件既不是私人的，也不是秘密的。它可以很容易地被複製、轉發、保存、攔截、存檔，並可能在訴訟中提出。電子郵件中不當評論的受眾可能是出乎意料的，而且非常普遍。

4.3 教職員切勿將學校網絡、互聯網或電郵用於以下用途：

- 虐待、誹謗、誹謗、騷擾或歧視（特別是但不限於性別、性取向、婚姻狀況、種族、膚色、國籍、民族或國籍、宗教、年齡、殘疾或工會會員資格）；
- 發送或接收淫穢或色情材料;
- 損害學校的聲譽或以可能使學校作為雇主感到尷尬的方式;
- 發送垃圾郵件或群發郵件或發送或接收連鎖郵件;
- 侵犯他人的版權或其他知識產權;
- 進行任何其他非法或不當行為;
- 未經許可，對外上傳或發布學校學生或教職員的圖像;或
- 侵犯他人隱私

4.4 對寄件者來說看似無害的電子郵件內容實際上可能會冒犯其他人。因此，教職員應注意，在判斷電郵是否屬於上述任何類別，或一般不合適時，學院會考慮電郵收件人的反應和敏感性。

4.5 如果員工透過電子郵件收到不適當的材料，則不應將其轉發給任何其他人。雖然工作人員阻止發送人不再發送此類性質的材料是適當的，但也可能要求向首席副校長（輔導）報告。

4.6 學校明白教職員不能總是控制發送給他們的訊息。但是，所有員工都必須阻止第三方（例如家人、朋友或同事）向他們發送不當信息。如果員工收到不適當的訊息或電子郵件附件，他或她必須：

a. 傳送訊息給傳送不適當電子郵件的人，指出不應傳送此類訊息。適當的回應如下所示：「
請不要再向我發送此類材料。本電子郵件的內容不符合學校的電子通信政策。你向我發送這封電子郵件違反了學校的政策，並使我面臨這樣做的風險。違反學院的電子通信政策將帶來嚴重後果。

b. 你不妨將此回覆的副本（連同不適當的訊息）轉發給首席副校長（輔導）和/或資訊及通訊科技署署長。

c. 刪除訊息。

4.7 不適合工作場所或學校環境的評論在通過電子郵件發送時也是不合適的。電子郵件很容易被誤解。因此，應仔細選擇文字和附件，並以清晰、專業的方式表達。

4.8 教職員應注意，以不符合本政策的方式或任何其他不當方式使用本校的資訊及通訊科技網絡，包括但不限於用於本政策第 4.3 段所述的用途，可能會引起紀律處分，包括終止僱傭關係或與承辦商的聘用。

4.9 未經適當個人授權，不得將內部電子郵件和其他內部資訊轉發至哈羅香港網域以外的目的地。

5. 資料保護和隱私

5.1 教職員在代表本校執行職務時，可能會查閱或處理與他人有關的個人資料，包括學生、同事、承辦商、住戶、家長及供應商。電子郵件不得用於披露他人的個人信息或關於他人的信息，除非根據學校的數據保護政策或獲得適當的授權。

5.2 資料保護法例要求教職員及學院採取合理措施，保護因受僱而持有的任何個人資料，免遭濫用及未經授權的存取。違反資料保護的行為可能會被學校視為嚴重不當行為，這可能導致即時解僱。因此，員工必須：

- 對其學校電腦以及他們因受僱而可能使用的任何個人電腦和可移動存儲設備（包括移動電話）的安全負責;

- 除非絕對必要，否則不得使用個人擁有的家用電腦、筆記型電腦或任何便攜式電子設備來儲存學校機密資料（例如學生/家長地址、 電子郵件地址、電話號碼、病歷、教職員資料等）；
- 如果需要將機密資料傳輸到學校以外的地方（透過電子郵件或互聯網，或使用可攜式儲存媒體，如記憶棒、CD、DVD、可攜式硬碟等），請採取一切合理的預防措施，並在不再需要資料時安全地刪除或銷毀資料;
- 如果學校的 ICT 部門需要有關適當安全措施的任何幫助或建議，請聯繫他們。

5.3 教職員被分配一個用戶名和密碼才能使用學校的電子通信設施，並且必須確保這些詳細信息不會向任何其他人披露，並採取措施確保這些詳細信息的安全。例如，強烈建議員工定期更改密碼，並確保其用戶名稱代碼和密碼不會以書面形式保存在其工作區域附近。

5.4 工作人員在離開辦公桌時應鎖定屏幕或註銷，並在夜間註銷並關閉計算機。這將避免他人未經授權存取教職員的個人資料、他人的個人資料和學院內部的機密資料。

5.5 為了遵守學校在資料保護立法下的義務，我們鼓勵教職員在向多個收件人發送電子郵件時使用盲件選項，因為披露這些人的電子郵件地址會侵犯他們的隱私。

5.6 除上述規定外，教職員亦應熟悉本校的資料保護政策，並確保他們使用電郵時不會違反資料保護法例。如果對符合數據保護法規有任何疑問，應該連絡合規性管理員。

5.7 不應使用自動轉發電子郵件的功能將訊息轉發到個人電子郵件帳戶，以確保學校資訊和數據的完整性。ICT 或許可以提供解決方案，以便在離開辦公室或需要遠端存取時存取哈羅香港的電子郵件系統。

6. 分銷和版權

6.1 當透過本校的電腦網絡或向本校以外的第三方分發資訊時，教職員必須確保他們和本校有權這樣做，並且沒有侵犯任何第三方的知識產權。

6.2 必須始終遵守可能適用於任何可能需要分發的資訊的版權法。未經特別授權，不得透過電子郵件分發第三方的版權資料（例如軟體、資料庫檔案、文件、卡通、文章、圖形檔案和下載資料）。類似的警告也適用於在學校網絡上發布學生照片。

6.3. 如果員工不確定是否獲得足夠的授權來分發資訊，請首先聯絡行銷與傳訊經理。

7. 機密性

7.1 由於互聯網和電子郵件是不安全的信息傳輸方式，因此不應通過電子郵件發送機密或敏感性質的項目：總會在某處有痕跡並保存副本，而不一定只保存在學校的網絡服務器上。

7.2 教職員必須確保從其學校電子郵件地址發送的所有電子郵件都包含學校的標準免責聲明訊息。此訊息將設定為自動出現在每封外寄電子郵件上。如果此功能不起作用，請聯繫 ICT 部門的成員。

7.3 存在錯誤歸屬電子郵件的風險。軟體隨處可見，可以透過這些軟體對電子郵件進行編輯或「篡改」，以反映錯誤的訊息或寄件者名稱。因此，收件人可能不知道他或她正在與冒名頂替者交流。對傳入電子郵件寄件者的身分保持合理的謹慎態度，並在有疑慮時透過其他方式驗證寄件者的身分，這一點始終很重要。

7.4 保留訊息會佔用網路上的大量儲存空間，並會降低效能。員工應盡量減少收件匣和寄件匣內的郵件，並定期刪除舊的或不必要的電子郵件。如果被告知超過個人電子郵件存儲限制，應聯繫 ICT 部門尋求幫助。

8. 社交媒體

8.1 學院認識到許多教職員在工作場所之外和正常工作時間之外以個人身份使用社交媒體。雖然他們在這種情況下不代表學校行事，但教職員必須意識到，如果他們在網上被識別為學校的教職員之一，他們仍然可能對學校造成損害。因此，學校制定嚴格的社交媒體規則來保護其地位非常重要。

8.2 在任何時候登入和使用社交媒體網站和網誌時，包括在工作場所外和正常工作時間之外個人使用非學校資訊及通訊科技設備時，工作人員不得:

- 以可能對學校有害或使學校或其學生、承包商、居民、家長和供應商聲譽受損的方式行事，例如發布不適當的圖像或視頻剪輯或指向不適當網站內容的鏈接。
- 允許他們在這些網站或博客上的互動損害與教職員與學生、同事、承包商、居民、家長和學校供應商之間的工作關係，例如，通過批評或與這些人爭論。
- 未經學校教職員、學生、同事、承辦商、住戶、家長或供應商明確同意，包括有關他們個人資料或資料（即使教職員、學生、同事、承辦商、住戶、家長或供應商在網站或部落格中沒有明確點名，只要學校合理地相信他們是可識別的，員工仍可能承擔責任）——這可能構成違反《資料保護法》的法例， 這是刑事犯罪。
- 對本校、其教職員、學生、承辦商、住戶、家長或供應商作出任何詆毀、冒犯、歧視、不實、負面、批評或誹謗的評論（即使本校、其教職員、學生、承辦商、住戶、家長或供應商在網站或網誌中沒有明確點名，只要本校合理地相信他們是可識別的，僱員仍可能承擔責任）。
- 對任何教職員發表任何可能構成非法歧視、騷擾或網絡欺凌的評論，違反平等機會法例，或發布任何歧視性或可能構成非法騷擾或網絡欺凌的圖片或影片片段，教職員須為其根據該法例的行為承擔個人責任。

- 披露屬於本校、其教職員、學生、同事、承辦商、住戶、家長或供應商的任何商業秘密或機密、專有或敏感資料，或任何可能被本校的一個或多個競爭對手使用的資料，例如有關本校工作、產品和服務、技術發展、正在進行的交易或未來業務計劃和員工士氣的資訊。
- 侵犯屬於學院的版權或任何其他專有權益，例如未經許可使用他人的圖像或書面內容，或在已獲准複製特定作品的情況下未給予確認。如員工希望在其網上個人檔案上發布其同事或學生、承辦商、居民、家長或供應商的圖像、照片或影片，應先獲得對方的明確許可。
- 教職員不應在互聯網（包括社交網站）上發表任何可能被視為代表哈羅香港、不符合學院價值觀和理念的個人意見或言論。

8.3 如果學校要求教職員刪除任何令人反感的內容，他們必須立即刪除。

8.4 員工應記住，即使他們已將帳戶隱私設置設置為限制訪問或"僅限朋友"級別，社交媒體網站也是公開的論壇，因此他們不應假設他們在任何網站上的帖子將保持私密。

8.5 員工在使用社交媒體網站時也必須有安全意識，並應採取適當措施保護自己免受身份盜用，例如將他們的隱私設置置於高水平，並限制他們提供的個人資料數量，例如出生日期和地點。此類資訊可能構成其他網站（例如網路銀行）上安全問題和/或密碼的基礎。

8.6 如果工作人員在網上發現有關學校的任何不准確信息，他們應首先向傳播主管報告。

9. 病毒

9.1 所有外部檔案和附件將使用掃描軟體自動進行病毒檢查。互聯網是計算機病毒的潛在宿主。從互聯網下載受感染的信息對學校計算機網絡可能是致命的。附加到傳入電子郵件的文件可能嵌入了病毒。

9.2 如果工作人員擔心電子郵件附件，或認為該附件沒有自動掃描病毒，則應聯繫 ICT 部門，而無需打開附件或回复電子郵件。

10. 員工使用內部電子郵件的指引

10.1 學校在快節奏且有時壓力很大的環境中運作，電子郵件被接受為日常使用的主要溝通方式之一。電子郵件可能是傳達特定訊息的最佳方式，但在數位資訊「超載」的時代，所有員工都應該注意過度電子郵件驅動的文化的影響，並就與他人溝通的內容、時間和方式做出明智的選擇。

10.2 隨著許多人現在透過多個個人和工作裝置存取電子郵件，以促進生產力和效率的方式適當使用電子郵件，同時使員工能夠管理合理的工作與生活平衡變得越來越重要。

10.3 雖然寄件者有權隨時發送電子郵件，但收件者也有權選擇何時閱讀收到的電子郵件，前提是這符合公認的專業行為水平，並符合對其角色和職責的期望。不應普遍期望員工會閱讀和回复深

夜發送的電子郵件，但預計所有電子郵件都會在收到後 24-48 小時內（學期期間）得到某種形式的回复——即使這只是一個等待回复。如果在周末收到電子郵件，可能需要快速回复或發送保留回复，並在下一個上學日發送完整回复。

10.4 就目前被認為是良好做法而言：

- 應始終使用專業稱呼和簽字，例如親愛的.....然後是最美好的祝願或親切的問候。如果兩個人之間出現電子郵件線索，則可以刪除問候。
- 在使用「全部回覆」之前請三思而後行，確保正確使用抄送，並考慮電子郵件的所有參與者是否需要在初次交流後繼續被抄送或包含在電子郵件追蹤中。
- 考慮電子郵件的語氣以及它可能傳達的方式——請記住，來自不同文化和背景的人可能會有不同的解釋。因此，最好避免諷刺、幽默或口語化，並儘可能清晰地寫作。
- 校對每封郵件，只有在電子郵件完成並檢查完畢後才添加電子郵件地址。這將防止任何電子郵件在編輯之前意外發送。
- 如果內容敏感，最好開會或打電話。然而，如果必須發送敏感郵件，則應在發送前大聲朗讀訊息，以確保語氣適當，避免誤解。
- 當教職員離開學校或長時間無法工作時，應使用自動「不在辦公室」通知。
- 沒有什麼是機密的 - 因此，請相應地寫作並始終保持尊重，有尊嚴地對待他人。
- 學校的社會願景：「一個充滿關懷、尊重的社區，讓每個人都茁壯成長」在我們的在線社區中同樣重要。

11. 一般事項

11.1 本政策中描述的條款和建議行為並非詳盡無遺，也不預期學校電子郵件和互聯網設施的每一種可能使用。我們鼓勵員工謹慎行事，並考慮本政策的基本原則。

11.2 此原則可能會變更，目前版本會張貼在員工內部網路 （SharePoint） 上。

Dinesh Alwani，ICT 總監
2024 年 8 月

聲明

本人認識到，當用戶在線時，服務器會記錄用戶的行為，並且任何明顯違反法律或學校規則的行為都可能受到調查。本人同意嚴重違反電腦使用規則的行為將作為紀律事項處理，並在適用的情況下，警方或地方當局可能會參與其中。

學校保留權利，就任何教職員保管的電腦設備的任何損失或損壞，如未獲保險索償，收取任何自負額。

本人理解學校的社會願景聲明：“一個充滿關懷、尊重的社區，讓每個人都茁壯成長”，並同意在本人的所有在線活動中遵守這一聲明。

本人已閱讀並充分理解上述條件，並同意遵守：

簽名

列印名稱

科

日期

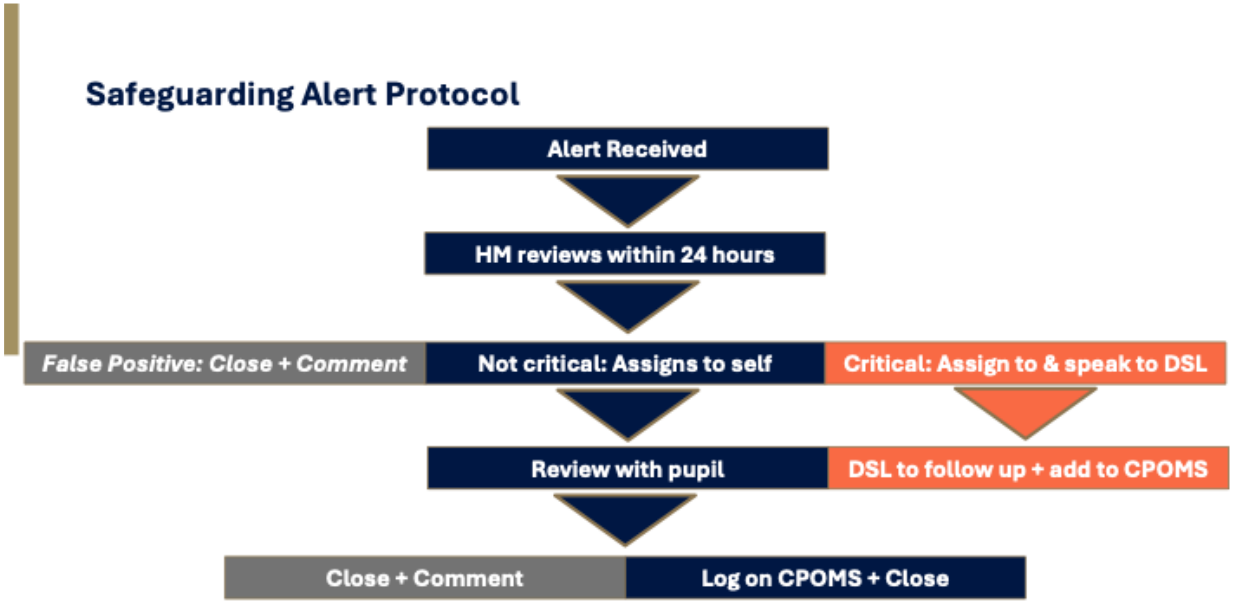
請簽名並交回人力資源總監

E. A. Haydon
校長

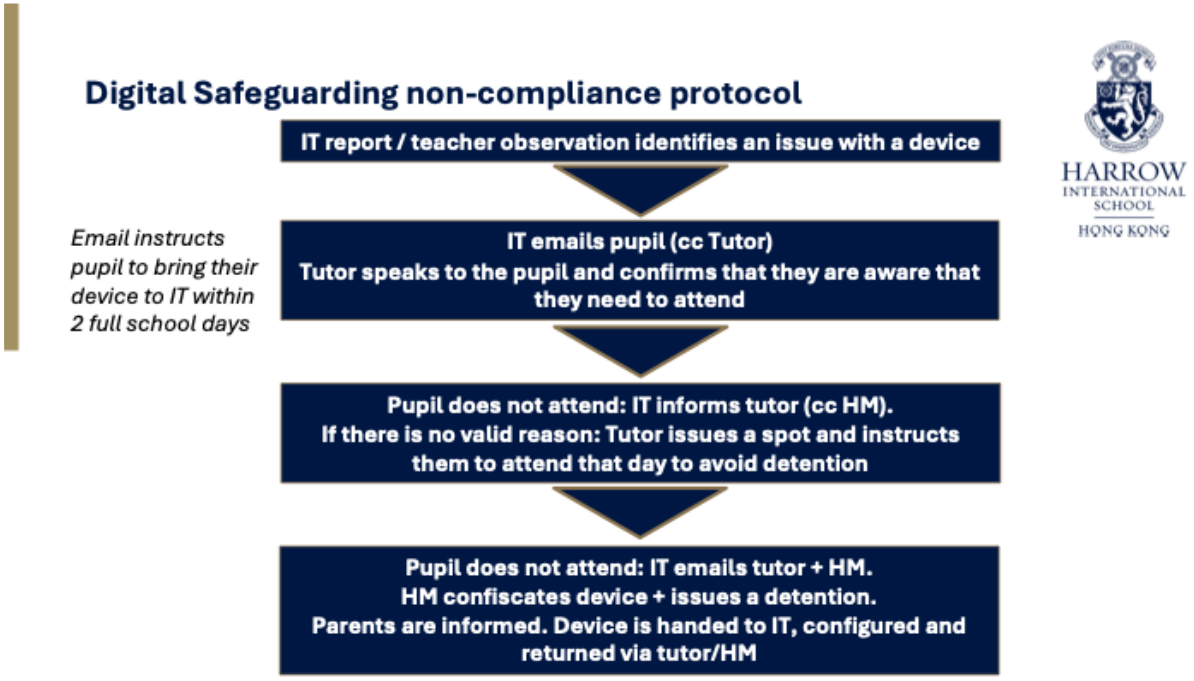
2024 年 8 月

評論日期：2024 年 7 月 31 日
下次評論：2025 年 8 月 1 日
所有者：信息通信技術總監

附錄 3：保障警示協議


Safeguarding Alert Protocol
Alert Received
HM reviews within 24 hours
False Positive: Close + Comment
Not critical: Assigns to self
Critical: Assign to & speak to DSL
Review with pupil
DSL to follow up + add to CPOMS
Close + Comment
Log on CPOMS + Close

附錄 4：數位保護不合規協議



附錄 5：數位安全回應協議

目的:

概述出現線上安全問題或事件時應採取的步驟。

回應步驟：

1. **報告：**
    a. 學生可以向老師、DSL 或其他值得信賴的成年人報告問題。
    b. 如果家長/監護人懷疑有問題，可以聯繫學校。
2. **調查：**
    a. DSL 將與 IT 和相關工作人員合作領導調查。
    b. 所有在線事件都會被記錄下來以供將來參考。
3. **行動：**
    a. 根據嚴重程度採取紀律處分，從警告到設備限制。
    b. 為受網絡欺凌或網絡虐待影響的學生提供支持和諮詢。
4. **跟進**:
    a. 與學生和家長進行跟進，以確保問題得到解決。

警戒 對過濾/監控問題的輔導回應的優先順序：

優先事項 1 - 立即回應

- 自殘/自殺相關內容
- 兒童保護/虐待材料
- 暴力的直接威脅
- 非法內容

優先事項 2 - 即日回應

- 網絡欺凌事件
- 不當內容存取
- 多次嘗試繞過安全性

優先級 3 - 48 小時響應

- 令人擔憂的行為模式
- 多次嘗試存取封鎖的內容
- 不尋常的瀏覽模式

優先事項 4 - 每週回顧

- 違反一般政策
- 生產力問題
- 資源的非教育用途

附錄 6：家長和監護人資源

目的：

為家長提供外部工具和資源，幫助確保孩子的上網安全。

主要資源：

- **線上安全資訊：**
    - 英國更安全的互聯網中心： https://saferinternet.org.uk/
    - Common Sense Media： https://www.commonsensemedia.org/
    - Internet Matters： https://www.internetmatters.org/
    - 家長資訊： https://www.educateagainsthate.com/resources/parent-info/
- **網路霸凌預防：**
    - StopBullying.gov： https://www.stopbullying.gov/
    - 國際 ChildNet： https://www.childnet.com/
    - Ditch the Label:： https://anti-bullyingalliance.org.uk/aba-our-work/our-members/core-members/ditch-label
    - Cybersmile 基金會： https://www.cybersmile.org/
- **家長監護和監控：**
    - 國家網路安全指南： https://nationalcollege.com/guides/what-parents-need-to-know-about-online-content-10-tips-to-keep-your-children-safe-online
    - OpenDNS： https://support.opendns.com/hc/en-us/articles/227988127-Getting-started-About-using-OpenDNS
    - Qustodio： https://www.qustodio.com/en/
    - 螢幕時間： https://support.apple.com/en-us/108806

附錄 7：詞彙表

目的:

定義政策中使用的技術和保護術語。

關鍵術語：

1. **學生安全：** 學生的安全和福祉。
2. **數位公民：** 學生負責任地使用技術，積極、安全地參與數位世界。
3. **正向數位文化：** 一種促進尊重、包容和負責任的線上行為的文化。
4. **數位風險：** 網路霸凌、隱私外洩和網路騷擾等網路危險。
5. **事件報告：** 報告和回應網路安全事件的程序。
6. **保障措施：**採取技術、教育和政策措施，保護學生免受線上風險。
7. **在線學習平台：** 用於在線學習活動的平台。
8. **個人設備：** 學生和教職員使用的筆記型電腦、平板電腦和其他設備。
9. **學校發放的設備：** 學校出於教育目的提供的設備。

附錄 8：LightSpeed 過濾和自動警報時間表

小學部學生

時段	程序	過濾	監控	警報
在學校規則中	上午 7：00 - 下午 4：30	開啟（LS **過濾**器）	在	在
校外規則	下午 4：30 - 上午 6：59 及非上課日	開啟（LS **過濾**器）	關閉	關閉

初中部日間學生

時段	程序	過濾	監控	警報
在學校規則中	上午 7：00 - 下午 4：30	開啟 （PS **過濾**）	在	在
校外規則	下午 4：30 - 上午 6：59 及非上課日	開啟 （OOS **過濾**）	關閉	關閉

初中部寄宿生

時段	程序	過濾	監控	警報
在學校規則中	上午 7：00 - 下午 4：30	開啟 （PS **過濾**）	在	在
	下午 4 時 30 分至早上 6 時 59 分	開啟 （OOS **過濾**）	在	關閉
校外規則	非上課日	開啟 （OOS **過濾**）	關閉	關閉

9 年級走讀生

時段	程序	過濾	監控	警報
在學校規則中	上午 7：00 - 下午 4：30	開啟 （Y9 **過濾**）	在	在
校外規則	下午 4：30 - 上午 6：59 及非上課日	開啟 （OOS **過濾**）	關閉	關閉

9 年級寄宿生

時段	程序	過濾	監控	警報
在學校規則中	上午 7：00 - 下午 4：30	開啟 （Y9 **過濾**）	在	在
	下午 4 時 30 分至早上 6 時 59 分	開啟 （OOS **過濾**）	在	關閉
校外規則	非上課日	開啟 （OOS **過濾**）	關閉	關閉

高中部走讀生

時段	程序	過濾	監控	警報
在學校規則中	上午 7：00 - 下午 4：30	開啟（SS **過濾**）	在	在
校外規則	下午 4：30 - 上午 6：59 及非上課日	開啟 （OOS **過濾**）	關閉	關閉

高中部寄宿生

時段	程序	過濾	監控	警報
在學校規則中	上午 7：00 - 下午 4：30	開啟（SS **過濾**）	在	在
	下午 4 時 30 分至早上 6 時 59 分	開啟 （OOS **過濾**）	在	關閉
校外規則	非上課日	開啟 （OOS **過濾**）	關閉	關閉

附錄 9：學生監察數據的資料保護及保存

1. **數據傳輸**

- 每週報告會以電子郵件中的 SharePoint 連結形式傳送，因此不存在資料傳輸風險

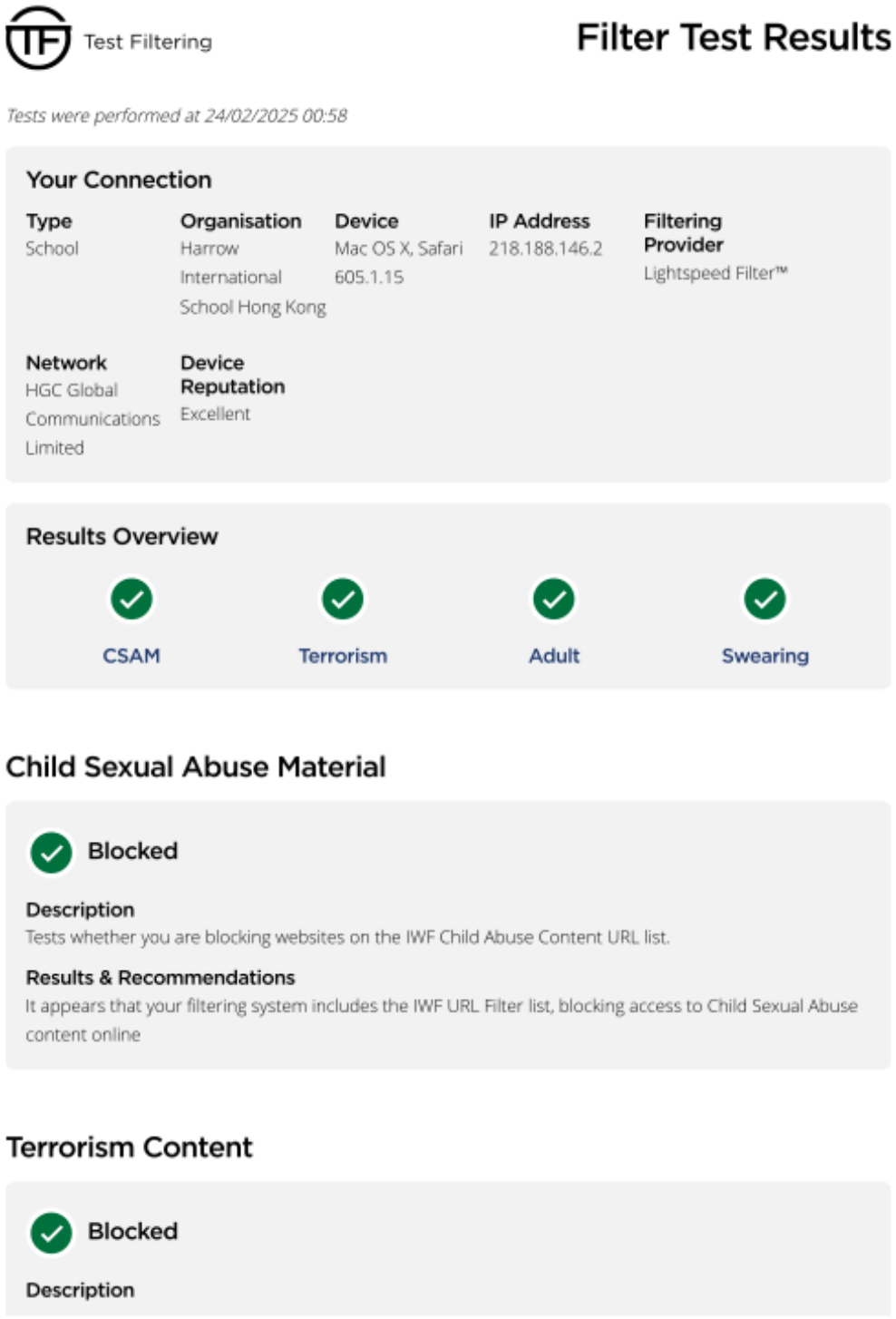
2. **資料儲存**

- 地點：SharePoint [家庭輔導團隊報告/文件/防火牆報告]
- 格式：加密資料庫，具有對特定個人的存取控制
- 備份：SharePoint 資料透過 M365 自動備份

3. **資料保留期限**

- 網路活動記錄：90 天
- 螢幕擷取：30 天
- 實時監測數據：60 天
- 警報記錄：90 天
- 防火牆報告：90 天

附錄 10：測試過濾結果


Test Filtering
Filter Test Results
Tests were performed at 24/02/2025 00:58
Your Connection
Type
School
Organisation
Harrow International School Hong Kong
Device
Mac OS X, Safari 605.1.15
IP Address
218.188.146.2
Filtering Provider
Lightspeed Filter™
Network
HGC Global Communications Limited
Device Reputation
Excellent
Results Overview
CSAM
Terrorism
Adult
Swearing
Child Sexual Abuse Material
Blocked
Description
Tests whether you are blocking websites on the IWF Child Abuse Content URL list.
Results & Recommendations
It appears that your filtering system includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online
Terrorism Content
Blocked
Description

Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

Results & Recommendations
It appears that your filtering system includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

Adult Content

Blocked

Description
Test whether your Internet filter blocks access to pornography websites

Results & Recommendations
It appears that your filtering system includes blocking for adult content. This indicates that your system has a list of adult websites or pages that are actively being blocked.

The test only checks to see if blocking is in place, and does not measure the effectiveness of the blocking across the range of available sources. Check with your filter provider that your system is setup in the most effective way, and matches your policy and needs.

Offensive Language

Blocked

Description
Accesses a page containing offensive language to test if your filtering software blocks it

Results & Recommendations
It appears that your filtering system includes blocking for offensive language

數位保障政政策数位保障政政策

HARROW INTERNATIONAL SCHOOL HONG KONG

1. 介绍

哈罗香港国际学校致力于为所有学生提供一个安全可靠的学习环境，无论是在实体课堂还是在数字世界中。 本数字保护政策旨在为学校社区的所有成员创造一个安全可靠的数字环境，并促进负责任的数字公民意识。

2. 关键原则

- **学生安全**：学生的安全和福祉是我们的首要任务。
- **正向数字文化**：我们提倡积极和负责任的数字文化，促进尊重和包容，符合学院的价值观和社会愿景。
- **数字素养教育**：我们对学生进行网络风险、网络霸凌、隐私和负责任的在线行为的教育。
- **事件报告**：我们有明确的报告和回应线上事件的程序。
- **协作**：我们与家长和监护人合作，确保线上安全。

我们方法的关键原则在数字保护政策信息图表**概述。**

3. 保障措施

为确保安全可靠的数字学习环境，哈罗香港国际学校实施了一套全面的保障措施。 这些措施包括数字素养教育计划、技术解决方案和政策，以保护学生免受网络风险并促进负责任的数字公民。

3.1 技术（移动设备策略）

- **Apple Classroom**：Apple Classroom 提供监控课堂活动摘要的平台，使教师能够保持学生参与度的概览，并透过所谓的实体监控来支持在线安全。 此外，它能够实时监控学生活动，使教师能够快速识别和解决任何不当或有风险的在线行为，从而有助于保护学生，确保学生在课堂上的数字学习体验中保持专注和安全。

- **LightSpeed 保护软件**：该工具集成了内容过滤、监控和机器学习扫描，通过有效监控和管理在线活动来创建安全的数字环境。 它在防止危险的线上行为方面发挥着至关重要的作用，并确保用户只能访问安全且经过批准的在线资源，从而降低暴露于可能危及数据安全的恶意网站或网络钓鱼尝试的风险。 LightSpeed 安装在所有注册学生拥有的 MacBook（高中）和 iPad（预科班和预科学校）以及学校拥有的设备上。 这种全面的覆盖范围确保了所有平台上一致的保护和监控。

    - **LightSpeed 过滤器：** LightSpeed 过滤器会阻止不适合学生使用的网站和应用程序。这包括通过应用程序、VPN 和网络共享到 4G/5G 热点的流量。

    - **LightSpeed 监视器：** LightSpeed 监视器提供有关学生在线活动的全面报告，包括在尝试访问已被封锁的网站时进行记录。

- **LightSpeed 警报**：LightSpeed Alert 扫描在线内容以查找自残、网络欺凌或暴力的警告信号，这些信号会转发给辅导领袖和学校的 DSL，以便及时干预。 通过这种方式，它在风险最高的情况下提供主动监控。

- **装置 MAC 地址过滤**：只有经注册学校的 MDM，Jamf Pro 的设备才能通过学校的 WiFi 网络访问网络。 以这种方式按设备过滤可确保只有配备所需软件的经批准的设备才能存取学校的 Wi-Fi。 这项措施是为了支持合规性，特别是在更换学生设备的情况下。

- **防火墙**：学校实施强大的防火墙系统，主动监控和阻止对不适当、恶意或非教育网站的访问。这包括与游戏、社交媒体、成人内容、代理服务器和其他潜在有害材料相关的内容。 该系统会产生全面的报告，详细说明尝试访问被封锁的网站，并由 ICT 部门和 DSL 进行审查。 ICT 部门审查匿名和汇总数据，以识别模式并根据需要调整过滤策略，DSL 审查与个别学生相关的问题。这种积极主动的方法可确保学生保持对教育内容的关注，同时保护他们免受线上威胁。 防火墙的智能分类系统会定期自动更新，以应对新的线上威胁并保持与学校教育目标的一致性。

- **透过学校的 MDM，Jamf Pro 停用管理员存取学生拥有的设备**：为了防止学生安装游戏或其他分散注意力的应用程序，所有 3 至 9 级的 MacBook 和 iPad 上都会停用管理员访问权限。 此外，Apple Store 隐藏在 iPad 上。 家长可以选择在孩子的装置上设定「家人共享」账户。 透过此设置，他们可以管理装置上安装的应用程序和程序，同时确保其符合学校的学习目标。

- **定期审核**：学校定期（至少每年）对技术工具进行审核，以确保它们保持有效和最新。

- **数据隐私合规性**：学校通过定期审查数据处理程序，确保遵守当地的数据保护法规。

- **设备预期使用情况和软件签入报告**： IT 监控设备的使用情况，以确保遵守保护软件的安装和维护。 例如，如果学生设法卸载 Jamf，它将向 IT 部门产生警报。 这些报告和警报在辅导团队的支持下引发调查。 详情请参阅附录 4，数码保障违规协议。

3.2. 寄宿公寓的定时 Wi-Fi 接入

为了促进健康的上网习惯、鼓励集中学习并确保充足的休息，寄宿公寓的 Wi-Fi 接入遵循时间表。 具体来说，WiFi 接入会在夜间关闭。 这项措施有助于平衡数字参与与线下活动，并促进健康的睡眠时间表。

- **初中宿舍（6-8 年級）**： Wi-Fi 在晚上 8：30 至早上 7：30 關閉。
- **高中宿舍（9-11 年級）**： 晚上 10：30 至早上 6：30 關閉 Wi-Fi。
- **预科宿舍（12-13 年级）**： Wi-Fi 在晚上 11：00 至早上 6：00 关闭。
  较晚的截止时间可以满足年龄较大的学生的学业需求，并允许稍微延长晚上的个人活动时间。

3.3 过滤和监控

在哈罗香港，我们使用过滤软件来限制对不当内容的访问，并监控学生设备上的线上活动，以确保负责任和安全的使用。 学生 ICT 行为准则定义了预期的在线行为，所有学生和家长/监护人在访问学校网络之前都必须同意它。

监控有两种形式：通过 LightSpeed 过滤器和网络防火墙记录尝试访问过滤站点，以及通过 LightSpeed 主动监控危害警告指标。

更新过滤器：如果网站被错误封锁，学生和教职员都可以向学校的 ICT 部门报告。 他们可以选择向 askit@harrowschool.hk 发送电子邮件 或填写 Microsoft 表格：点击这里。 这确保了快速解决存取问题，保持对线上资源的顺利、不间断的访问。

监控系统的任何变更都会经过审批流程并记录下来，从而实现审计跟踪，确保透明度，并且个人无法进行单方面更改。

为确保我们的筛选规则适当，我们会定期审查和更新这些规则。 英国更安全的互联网中心获得认可 测试过滤实用器 至少每年用于审查学校的过滤规则。
见附录 8。

3.4 线上活动的报告和监控

哈罗香港加强了线上活动的报告和监控协议。 这些协议确保通过防火墙和 LightSpeed 系统收集的数据得到有效和负责任的审查和使用，以维护学生的安全和福祉，同时遵守《个人资料（隐私）条例》（PDPO）。

3.4.1 防火墙报告和辅导团队的审查

学校的防火墙系统会产生有关尝试访问被封锁网站和其他受限制线上活动的详细报告。 这些报告由辅导团队根据以下准则进行审查：

a. 数据范围：
- 报告将尽可能包含匿名或汇总数据，重点关注不当访问尝试的模式。
- 对于已识别的事件，可能会访问特定用户数据（例如设备识别码、时间戳记和 URL）来调查违反学生 ICT 行为准则的行为。

b. 访问控制：
- 防火墙报告通过安全访问链接发送，只有辅导团队的授权成员才能访问。

c. 目的：
- 识别不当线上行为的趋势，并相应地调整政策和教育。
- 解决学生试图存取有害或不当内容的个别事件。

d. 频率：
- 资讯及通讯科技部门每周向辅导团队提供防火墙活动摘要。
- 重大事件（例如，尝试访问成人内容或恶意网站）的即时警报将立即升级。

3.4.2 LightSpeed 辅导团队的报告和审查

LightSpeed 提供先进的监控功能，包括针对自残、网络霸凌或暴力等危险线上行为的警报。 下列协议将会控管数据的使用：

a. 数据范围：
- LightSpeed 根据预先定义的风险指标产生警报，包括标记的关键词、异常浏览活动、屏幕撷取报告和监控活动日志。
- 开启监控后，系统会收集 Web 活动数据，包括 URL 访问记录、浏览持续时间、网站类别、下载活动、搜索查询、带宽使用情况、带时间戳记的 Web 会话和浏览器信息。
- 所有警报和报告都包含基本标识符，例如设备信息、用户配置文件、时间戳记和标记内容，以及屏幕监控数据，包括屏幕截图捕获、活动时间表和应用程序使用日志。

为遵守香港《个人资料（私隐）条例》（《私隐条例》），系统遵守特定的资料保留期限：网络活动日志保存 90 天，截图保存 30 天，实时监控数据保存 60 天，警报记录保存 90 天。

b. 辅导领袖的监督责任：

- 访问尝试分析 – 审查访问被封锁数据的频繁尝试，监控试图规避过滤系统的模式，并追踪对特定类别关注的重复访问尝试。
- 高风险内容监控 - 审查访问有害或危险材料的尝试，监控与自残、暴力或极端主义相关的搜索，并跟踪对不适合年龄的内容的访问尝试。
- 行为模式分析 - 审查搜索和浏览模式所花费的时间，监控在线活动的异常时间，并跟踪可能表明问题的典型使用模式的变化。
- 政策合规性 - 确保遵守可接受的使用政策、监控学校设备政策的合规性并跟踪教育资源的适当使用

审查和响应频率：
- LightSpeed 门户网站向辅导团队（年级领导、社监 和 DSL）提供 LightSpeed 警报的摘要。
- 关键警报会在检测到后一小时内自动发送给 DSL 和辅导领袖。
- 高优先级警示必须每天审查，并在当天收到回应。
- 有关更多详细信息，请参阅附录 3。
- 标准过滤器报告将每周审查一次。
- 应定期进行趋势分析。

d. 访问控制：
- 对 LightSpeed 报告的访问仅限于辅导团队。
- 针对保护问题的警报会直接发送给指定保障负责人（DSL）以立即关注。
- 对 LightSpeed 资料的所有访问都是通过受限权限、密码保护和记录的，并定期进行审核以确保遵守访问策略。

e.目的：
- 及时采取干预措施以保护问题，例如识别有受到伤害风险的学生。
- 通过解决不当的在线行为来支持学校的行为政策。
- 透过确保专注且安全的数字学习环境来提高教育成果。

3.5 访问数据和角色

根据《个人资料（PDPO）》和数据最小化和目的限制的原则，对防火墙和 LightSpeed 数据的访问受到基于角色的权限的严格管理：

1. 具有访问权限的角色：
- ICT 辅导联络： 负责管理和维护防火墙和 LightSpeed 系统并生成报告。 ICT 辅导联络员无法访问学生数据，但有助于为辅导团队生成和传播报告。
- 学生的辅导领袖（高年级的宿生家长和低年级的年级领导）：有权审查与学生保护和行为管理相关的报告和警报。
- 指定保护负责人 （DSL） 负责：
    - 监控和审查 LightSpeed 在所有年级组中生成的自动保护警报
    - 管理任何标记的保护问题的调查过程
    - 高级领导团队（SLT）： 可以访问汇总和匿名数据，以进行战略决策和政策更新。

2. 数据类别：
- 汇总数据：用于趋势分析和政策调整（例如，识别被阻止的网站访问模式）。
- 可识别数据：仅在调查特定事件、行为或保护问题时访问。

3. 访问协议：
- 所有对数据的访问都会被记录下来并接受定期审计。
- 有权访问的员工必须完成有关资料保护和保护协议的年度培训。
- 未经授权的访问或滥用数据将根据学校的政策受到纪律处分。

3.6 资料的使用

通过防火墙和 LightSpeed 系统收集的数据仅用于以下目的，符合《个人资料（私隐）条例》：

9. 保护学生：
    a. 侦测并应对网络霸凌、自残或接触有害内容等风险。
    b. 支持 DSL 和辅导团队提供及时的干预。
10. 行为管理：
    a. 监控学生 ICT 行为准则的遵守情况。
    b. 通过学校的行为政策解决不当的在线行为。
11. 政策制定：
    a. 识别线上活动的趋势，为数字保护政策和过滤规则的更新提供信息。
    b. 根据新出现的风险加强学校的数字素养课程。
12. 教育支持：
    a. 确保学生在数字学习活动期间专注于教育内容。
    b. 促进积极、安全的数字学习环境。

3.7 遵守香港《私隐条例》

香港哈罗国际学校通过遵守以下原则，确保所有数据收集、存储和处理活动都符合《私隐条例》：

11. **资料最小化**：仅收集保护、行为管理和教育目的所需的资料。
12. **目的限制**：资料仅用于本政策中概述的目的，不会与未经授权的各方共享。
13. **透明度**：学生、家长和教职员了解通过防火墙和 LightSpeed 系统收集的数据及其预期用途。
14. **安全性**：数据安全存储，存取仅限授权人员，并受到强大的技术保护措施的保护。
15. **保留**：数据仅在实现其预期目的所需的时间内保留，此后将安全删除。

3.8. 数字素养教育

哈罗香港确保我们所有学生的教育都包括保持上网安全并保障他们福祉所需的数字知识和技能。 这是数字素养课程的一个组成部分，通过低年级的计算机课程以及高年级的计算机科学课程和 PSHE 课程的组合进行教授。 所教授的组成部分符合英国政府的「互联世界教育」框架，并在数字策略政策中进行了详细说明。 学生数字安全指南包括具体提及 4C 带来的在线威胁：内容、联系、行为和商业。

家长网络研讨会：学校每年为家长提供网络研讨会，帮助他们了解一些必要的数字素养技能以及他们可以在家中做些什么来支持他们的孩子。

3.9 保护和人工智能

生成式 AI 工具对学生的福祉构成特定且重大的保护风险，包括但不限于接触有害内容，包括 AI 生成的儿童性虐待材料 （AI-CSAM）、霸凌、诱骗和骚扰。 此外，滥用个人资料可能会导致隐私外泄、产生虚假或误导性信息，并增加网络攻击、诈欺和诈骗的风险。 未经授权使用受版权保护的数据可能会导致知识产权问题，人工智能系统中现有偏见的延续或放大可能会导致不公平待遇或歧视。

我们致力于确保安全和负责任地使用人工智能技术，我们的措施在我们的人工智能政策中进行了概述。这些包括：

- **人工智能素养教学** 作为数字素养课程的一部分
- **默认情况下，生成式 AI 工具作为预备学校和预备学校中** LightSpeed 过滤规则的一部分被阻止
- **所有生成式 AI 应用程序在解锁和**/或在课堂上使用之前都会经过彻底的风险评估，以评估其益处和潜在风险，确保遵守数据保护、儿童安全和知识产权法等法律责任。

3.10 手机和不受限制的互联网访问

移动电话提供离散、不安全和不受监控的互联网访问，因此降低风险是本政策的一个特别考虑因素。使用移动或个人便携式 5G 路由器将移动设备（iPad 或 MacBook）连接到互联网而无需通过我们的网络过滤器的能力增加了这种风险。 本政策通过多种方式解决此问题：

- **上课时间手机使用限制：** 严格限制在校园内携带和使用手机。
- **旅行期间使用手机的限制：** 低年级和预科学校的学生不应使用手机，除非获得特别许可，这包括 SCA 和固定装置等场外活动。 高年级学生可以在旅途中和正式休息期间使用设备。 过夜旅行应遵守以下登机手机使用政策，或者如果旅行性质需要保持无手机环境。 更多详细信息请参阅旅行和参观政策。
- **使用网络共享的限制：**以确保在校期间的在线活动受到保护。 禁止与手机或便携式 5G 路由器进行网络共享，这包含在学生每年签署的《学生 ICT 行为准则》中。
- **LightSpeed 代理继续保护移动宽带**：作为设备上安装的软件，对于 MacBook（高中）和受监督的 iPad（Pre-Prep 和 Prep School），LightSpeed 即使在网络共享到手机时也会继续过滤和监控互联网活动。
- **透过 Jamf MDM 进行抽查**：IT 部门每天至少在连接到非学校网络的受管理设备上产生 3 次自动报告。 辅导团队使用这些信息来解决不合规问题。
- **晚上寄宿生手机使用和系留限制：**晚上寄宿生使用手机受到管理。 9 年级和 10 年级的高年级寄宿生在晚餐和准备时间下午 6.30 至晚上 8.30 交出手机。 他们可以在晚上 8 点 30 分领取手机联系家长，直到晚上 8 点 45 分。 所有手机和设备均在晚上 8 点 45 分至早上 7 点 45 分之前在 9 年级和 10 年级之前上交。 对于 11 年级，电话和设备在晚上 9.30 至次日早上 7.45 之间通宵上交。在下午 5.30 至 6 点之间，**初中部学生可以使用手机。** 寄宿生可以在每天晚上 7.30 至晚上 7.45 之间使用 6 年级和 7 年级的电话给家长打电话。 8 年级寄宿生可以在晚上 8.15 至晚上 8.30 之间使用手机。 所有电话和设备都经过夜间保护，直到第二天早上 7.30 这得到了家庭辅导团队的物理监控和 IT 网络共享报告的支持。

4. 事件报告和回应

4.1 防火墙和 LightSpeed 报告

防火墙和 LightSpeed 系统产生的报告将整合到学校的事件回应流程中，如下所示：

报告：

5. 来自 LightSpeed 的关键警报（例如，自残指标）会立即上报到 DSL。
6. 涉及反复尝试存取受限制内容的防火墙事件将被标记为辅导团队进行调查。

4.2 学生报告

- **报告**：鼓励学生向值得信赖的成年人报告网络安全问题，例如教师、HM 或指定保护负责人（DSL）。
- **匿名报告**：学校提供了一个安全的在线表格，可通过学校内联网访问，用于匿名报告数字安全问题，该表格直接路由到 DSL。

4.3 数字安全回应协议

学校通过其行为政策处理在线事件，其中包括调查程序、纪律措施以及对相关学生的支持。

- DSL 与 ICT 部门和相关工作人员合作领导调查。
- 纪律措施和支持计划是根据学校的行为和保障政策实施的。

4.4 回应及时性

学校对所有报告的事件保持严格的响应时间表，并按严重程度分类。 重大事件（危及生命）需要立即关注，必须在报告后一小时内解决，而其他问题则在 48 小时内迅速处理，以确保对所有案件给予适当关注。 在整个事件管理过程中，相关利益相关关系人会定期收到有关报告问题的进度和解决方案的状态更新。 信息及通信科技部门和高级管理层每月都会审查这些回应协议的有效性，以维持和改进服务标准，确保以最佳方式处理所有安保和安全问题。

4.5 说明文件

所有事件均会记录在案，并保留数据日志以作审计之用，以符合《私隐条例》的规定。

5. 员工职责

- **培训**：所有员工都接受有关数字保护程序及其在促进安全线上环境方面的作用的培训。
- **监控和报告**：辅导团队监控学生的在线活动，并向 DSL/DDSL 报告任何问题。
- **负责任的行为建模**：员工按照员工 IT 可接受使用政策（每年阅读并签署）塑造负责任的数字行为。
- **与家长沟通**：辅导团队定期与家长沟通网络安全，并就如何应对家庭数字风险提供指导。

6. 父母的责任

- **沟通**：鼓励家长定期与孩子讨论网络安全，并对负责任的线上行为建立明确的期望。
- **监控**：鼓励家长监控孩子的在线活动并确保安全的网络使用。
- **协作**：敦促家长表达对孩子线上安全的担忧，并与学校合作解决这些问题。
- **资源**：学校为家长提供资源，让他们随时了解网络安全问题，包括信誉良好的网络安全网站和工具的链接。

7. 审查和更新

哈罗香港致力于确保这项政策保持有效、相关，并与技术进步、新兴的网络威胁和不断变化的保障需求保持一致。 审查过程旨在通过学校社区的协作和反馈来促进持续改进。

7.1 定期检讨及谘询

- **年度审查**：本政策将进行年度审查，以确保其符合最新的保护措施、技术发展以及遵守香港个人资料（私隐）条例（PDPO）。
- **利害关系人咨询**：
  - 将积极寻求包括教职员、学生、家长和州长在内的主要利益相关者的反馈，以确保该政策反映学校社区的多样化需求。
  - 咨询过程可能包括调查、研讨会、焦点小组和非正式讨论，以收集有价值的见解和建议。
- **事件数据分析**：将分析来自防火墙和 LightSpeed 报告系统的数据以及事件日志，以识别趋势、评估当前措施的有效性并解决任何反复出现的问题。

7.2 报告协议的有效性

- 防火墙和 LightSpeed 报告协议的有效性将在年度政策评估期间进行专门审查。
- ICT 部门、辅导团队和指定保护负责人 （DSL） 的反馈将用于评估和提高监控、报告和响应流程的效率。
- 将及时实施改进建议，以维持健全的保护框架。

7.3 政策可访问性

- 学校网站上提供了关键保护措施的摘要，包括报告协议和数字素养指南，以确保清晰度和理解。

7.4 持续回馈机制

- 反馈机制允许利益相关者就政策提供持续的意见。
- DSL 和 ICT 部门将定期审查反馈，以确保及时更新和改进。
- 我们的数字保护政策通过结构化的反馈渠道保持有效性，使利益相关方能够参与并及时改进。

7.5 社群参与

- 为家长举办的学期 PGCG 会议和学院代表会议，以及家长网络研讨会和信息晚会
- 学生会会议、学生数字级长和社制数字代表
- 通过导师时间和学生数字级长的学生声音
- 部门会议上的员工咨询

7.6 动态更新

- 政策将根据需要进行更新，以解决以下问题：
- 新的线上风险或保障挑战。
- 当地法规的变化，例如《私隐条例》的更新。
- 技术进步或采用新的保护工具。
- 如有需要，将通过官方渠道（包括电子邮件通知和学校网站）及时向利害关系人传达中期更新。

7.7 透明度和问责制

- 该政策的所有更新都将被记录下来，并向利益相关者提供更改摘要以提高透明度。
- 高级领导团队 （SLT）将监督审查过程，以确保问责制并与学校的保护目标保持一致。

7.8 在幼儿中心使用流动电话

不得在幼儿中心内任何地方有儿童在场的情况下使用手机（紧急情况除外）。
只能使用学校拥有的数码设备拍摄学生及其学习的照片和/或视频。

8. 附录

- **附录一**：学生资讯及通讯科技行为守则
- **附录 2**：员工 ICT 可接受使用协议
- **附錄三**：保障警示協議
- **附录 4**：数字保护不合规协议
- **附录 5**： 数字安全回应协议
- **附录 6**：家长和监护人的资源（例如，网络安全网站的链接）
- **附录 7**：术语表
- **附录 8**：Lightspeed 配置设置
- **附录 9**：资料保护和保留
- **附录 10**：测试过滤结果

评论日期：2025年9月
下一篇评论：2026年8月
拥有人： 助理校长（数码策略、评估及追踪）
版本：2

附录 1：学生资讯及通讯科技守守则（2024/25）[高年级]

链接在这里： 学生 ICT 行为准则 2025-26

HARROW INTERNATIONAL SCHOOL HONG KONG

2025-26 年低年级学生数字行为准则

学校有责任确保香港哈罗国际学校的每位学生安全、负责任地使用数码设备、互联网和通讯设备。 在使用设备之前，所有学生都必须阅读、理解并签署本行为准则。 这适用于使用任何连接到学校网络的设备，包括 iPad、MacBook 和其他数字设备。

1. 学生不得使用他人账户或让自己的账户被他人使用。
2. 除非老师指示，否则学生不应通过互联网或任何其他方式相互发送信息。
3. 未经许可，学生不得分享有关学校或学校中任何个人的任何个人信息，例如文字或图像。
4. 学生不应尝试访问、发送或存储任何不适当的信息，包括图像。
5. 使用设备（包括 iPad）时，所有学生都必须遵守 iPad 黄金法则，如下所示和在教室中。

如果未履行上述协议之一，教师有权限制学生使用其设备。

我已阅读并理解小学部数码行为准则，并同意始终遵守这一点。

学生签名：_____

北京时间_____

附录 2： 员工信息及通讯科技可接受使用协议 （2024/25）

本文件规定了香港哈罗国际学校的所有教职员在使用任何设备进行电子通讯或使用学校的信息通信技术设施时应遵守的安全、管理和内部规则。 所有教职员均应密切留意本政策的条款，以尽量减少因滥用电邮或互联网设施而可能对自己、学生及学校造成的潜在困难。 本政策适用于本校所有员工、员工的常住家庭成员或任何其他使用学校信息及通讯科技设施的客人。

学校网络可供整个学校社区使用，包括学术和教育支持人员、学生、家长和访客，学校有责任确保哈罗香港的每位用户负责任地使用电脑设备和互联网，以及手机和其他通讯设备。 用户应期望他们在学校网络上的电脑使用受到监控，尽管这将是相称的，即仅在必要的情况下，并且以限制对隐私的潜在侵犯的方式进行。 所有用户都应在支持学校愿景声明、目标和目标的活动中使用学校的 ICT 系统、资源和相关应用程序。 因此，信息及通讯科技资源不得用于任何非法或不道德的目的，并应尽量减少娱乐或个人用途。 同样，用户不应从事任何可能破坏网络有效运行的活动。

1. 学校财产

1.1 学院认可并欢迎教职员在制作和储存教材方面的创造力，以支持教学、学习和管理。 值得注意的是，根据法律条文，员工、承包商和居民在履行正常职责时在学校网络上创建和储存的文件和电子邮件在技术上仍然是学校的财产。 如对版权及知识产权有任何疑问，我们鼓励员工征询处长的意见。

1.2 根据本政策中概述的进一步规定，**教职员、承包商和居民在学校网络上建立和存储的供其私人和个人使用的文件和电子邮件仍然是创建者的财产。**

2. 监控

2.1 本校的电脑网络是一种商业和教育工具，主要用于商业或教育目的。 因此，员工有责任以适当、专业和合法的方式使用这些资源。

2.2 学校系统上的所有信息和文件都将被视为与教育或业务相关的讯息和文件，并可能受到监控。因此，教职员不应期望在学校电脑网络上传输或储存的任何信息或文件是完全私密的。

2.3 教职员亦应注意，学院设有自动监察及过滤互联网使用情况的系统，包括教职员浏览的网站和内容，以及他们使用互联网的时间长短。

2.4 **教职员应认识到，如果担心可能被滥用，学校可能需要检查其内容，从而在编写电子邮件时认识到。**

2.5 电子邮件将由学校在认为适当并符合法定要求的情况下存档。

3. 个人使用

3.1 教职员可透过学校网络使用互联网及电邮设施收发个人资料，但须尽量减少使用，且不得妨碍其执行工作。

3.2 但是，出于个人目的使用学校网络仍受本政策中其他描述的相同条款和条件的约束，无论它是标记为私人还是机密。

3.3 在共享资讯科技设施的情况下，员工应尊重同事的需求，并及时有效地使用电脑资源。

3.4 在工作时间内出于个人原因过度或不当使用电子邮件或互联网设施可能会导致纪律处分。 例如，未经信息及 ICT 总监同意，**教职员不得下载大型视频**/音频档案供个人使用，亦不得下载大量影像，亦不得下载或安装电脑程序。

3.5 在任何时候，哈罗香港员工都应以最适当的方式进行网络通信，避免任何可能损害他们或学院声誉的互联网行为。

3.6 教职员不应使用社交网站或个人电邮账户与在校学生沟通。

4. 内容

4.1 电子邮件通信应与任何其他通信（例如信件或传真）相同：作为永久书面记录，收件人以外的人可以阅读，并可能导致个人或学校承担责任。

4.2 教职员及/或本校可能须对电邮内容负责。 因此，任何员工都不应使用他人的账户发送电子邮件，除非在紧急情况下，并且明确说明该电子邮件来自谁。 所有信息及通讯科技用户在不使用电脑时，应注销或锁定电脑。 电子邮件既不是私人的，也不是秘密的。 它可以很容易地被复制、转发、保存、拦截、存档，并可能在诉讼中提出。 电子邮件中不当评论的受众可能是出乎意料的，而且非常普遍。

4.3 教职员切勿将学校网络、互联网或电邮用于以下用途：

- 虐待、诽谤、诽谤、骚扰或歧视（特别是但不限于性别、性取向、婚姻状况、种族、肤色、国籍、民族或国籍、宗教、年龄、残疾或工会会员资格）;
- 发送或接收淫秽或色情材料;
- 损害学校的声誉或以可能使学校作为雇主感到尴尬的方式;
- 发送垃圾邮件或群发邮件或发送或接收连锁邮件;
- 侵犯他人的版权或其他知识产权;
- 进行任何其他非法或不当行为;
- 未经许可，对外上传或发布学校学生或教职员的图像; 或
- 侵犯他人隐私

4.4 对发件人来说看似无害的电子邮件内容实际上可能会冒犯其他人。 因此，教职员应注意，在判断电邮是否属于上述任何类别，或一般不合适时，学院会考虑电邮收件人的反应和敏感性。

4.5 如果员工通过电子邮件收到不适当的材料，则不应将其转发给任何其他人。 虽然工作人员阻止发送人不再发送此类性质的材料是适当的，但也可能要求向首席副校长（**辅导**）报告。

4.6 学校明白教职员不能总是控制发送给他们的讯息。 但是，所有员工都必须阻止第三方（例如家人、朋友或同事）向他们发送不当信息。 如果员工收到不适当的讯息或电子邮件附件，他或她必须：

a. 传送讯息给传送不适当电子邮件的人，指出不应传送此类讯息。 适当的回应如下所示：「
请不要再向我发送此类材料。 本电子邮件的内容不符合学校的电子通信政策。 你向我发送这封电子邮件违反了学校的政策，并使我面临这样做的风险。 违反学院的电子通信政策将带来严重后果。

b. 你不妨将此回复的副本（连同不适当的信息）转发给首席副校长（**辅导**）和/或信息及通讯科技署署长。

c. 删除讯息。

4.7 不适合工作场所或学校环境的评论在通过电子邮件发送时也是不合适的。 电子邮件很容易被误解。 因此，应仔细选择文字和附件，并以清晰、专业的方式表达。

4.8 教职员应注意，以不符合本政策的方式或任何其他不当方式使用本校的信息及通讯科技网络，包括但不限于用于本政策第 4.3 段所述的用途，可能会引起纪律处分，包括终止雇佣关系或与承办商的聘用。

4.9 未经适当个人授权，不得将内部电子邮件和其他内部信息转发至哈罗香港域以外的目的地。

5. 数据保护和隐私

5.1 教职员在代表本校执行职务时，可能会查阅或处理与他人有关的个人资料，包括学生、同事、承办商、住户、家长及供应商。 电子邮件不得用于披露他人的个人信息或关于他人的信息，除非根据学校的数据保护政策或获得适当的授权。

5.2 资料保护法例要求教职员及学院采取合理措施，保护因受雇而持有的任何个人资料，免遭滥用及未经授权的存取。 违反资料保护的行为可能会被学校视为严重不当行为，这可能导致即时解雇。 因此，员工必须：

- 对其学校电脑以及他们因受雇而可能使用的任何个人电脑和可移动存储设备（包括移动电话）的安全负责;
- 除非绝对必要，否则不得使用个人拥有的家用电脑、笔记本电脑或任何便携式电子设备来储存学校机密资料（例如学生/家长地址、 电子邮件地址、电话号码、病历、教职员资料等）;
- 如果需要将机密数据传输到学校以外的地方（透过电子邮件或互联网，或使用便携式存储媒体，如记忆棒、CD、DVD、便携式硬盘等），请采取一切合理的预防措施，并在不再需要数据时安全地删除或销毁数据;
- 如果学校的 ICT 部门需要有关适当安全措施的任何帮助或建议，请联系他们。

5.3 教职员被分配一个用户名和密码才能使用学校的电子通信设施，并且必须确保这些详细信息不会向任何其他人披露，并采取措施确保这些详细信息的安全。 例如，强烈建议员工定期更改密码，并确保其用户名称代码和密码不会以书面形式保存在其工作区域附近。

5.4 工作人员在离开办公桌时应锁定屏幕或注销，并在夜间注销并关闭计算机。 这将避免他人未经授权存取教职员的个人资料、他人的个人资料和学院内部的机密资料。

5.5 为了遵守学校在资料保护立法下的义务，我们鼓励教职员在向多个收件人发送电子邮件时使用盲件选项，因为披露这些人的电子邮件地址会侵犯他们的隐私。

5.6 除上述规定外，教职员亦应熟悉本校的数据保护政策，并确保他们使用电邮时不会违反资料保护法例。 如果对符合数据保护法规有任何疑问，应该连络合规性管理员。

5.7 不应使用自动转发电子邮件的功能将信息转发到个人电子邮件帐户，以确保学校信息和数据的完整性。 ICT 或许可以提供解决方案，以便在离开办公室或需要远程访问时访问哈罗香港的电子邮件系统。

6. 分销和版权

6.1 当透过本校的计算机网络或向本校以外的第三方分发信息时，教职员必须确保他们和本校有权这样做，并且没有侵犯任何第三方的知识产权。

6.2 必须始终遵守可能适用于任何可能需要分发的信息的版权法。 未经特别授权，不得通过电子邮件分发第三方的版权资料（例如软件、数据库档案、文件、卡通、文章、图形文件和下载资料）。 类似的警告也适用于在学校网络上发布学生照片。

6.3. 如果员工不确定是否获得足够的授权来分发信息，请首先联络行销与传讯经理。

7. 机密性

7.1 由于互联网和电子邮件是不安全的信息传输方式，因此不应通过电子邮件发送机密或敏感性质的项目：总会在某处有痕迹并保存副本，而不一定只保存在学校的网络服务器上。

7.2 **教职员必须确保从其学校电子邮件地址发送的所有电子邮件都包含学校的标准免责声明讯息。 此讯息将设定为自动出现在每封外寄电子邮件上。 如果此功能不起作用，请联系** ICT 部门的成员。

7.3 存在错误归属电子邮件的风险。 软件随处可见，可以通过这些软件对电子邮件进行编辑或「篡改」，以反映错误的讯息或发件人名称。 因此，收件人可能不知道他或她正在与冒名顶替者交流。 对传入电子邮件寄件人的身份保持合理的谨慎态度，并在有疑虑时通过其他方式验证寄件人的身份，这一点始终很重要。

7.4 保留讯息会占用网络上的大量存储空间，并会降低效能。 员工应尽量减少收件箱和寄件箱内的邮件，并定期删除旧的或不必要的电子邮件。 如果被告知超过个人电子邮件存储限制，应联系 ICT 部门寻求帮助。

8. 社交媒体

8.1 学院认识到许多教职员在工作场所之外和正常工作时间之外以个人身份使用社交媒体。 虽然他们在这种情况下不代表学校行事，但教职员必须意识到，如果他们在网上被识别为学校的教职员之一，他们仍然可能对学校造成损害。 因此，学校制定严格的社交媒体规则来保护其地位非常重要。

8.2 在任何时候登入和使用社交媒体网站和网志时，包括在工作场所外和正常工作时间之外个人使用非学校信息及通讯科技设备时，工作人员不得：

- 以可能对学校有害或使学校或其学生、承包商、居民、家长和供应商声誉受损的方式行事，例如发布不适当的图像或视频剪辑或指向不适当网站内容的链接。
- 允许他们在这些网站或博客上的互动损害与教职员与学生、同事、承包商、居民、家长和学校供应商之间的工作关系，例如，通过批评或与这些人争论。
- 未经学校教职员、学生、同事、承办商、住户、家长或供应商明确同意，包括有关他们个人资料或资料（即使教职员、学生、同事、承办商、住户、家长或供应商在网站或部落格中没有明确点名，只要学校合理地相信他们是可识别的，员工仍可能承担责任）——这可能构成违反《资料保护法》的法例， 这是刑事犯罪。

- 对本校、其教职员、学生、承办商、住户、家长或供应商作出任何诋毁、冒犯、歧视、不实、负面、批评或诽谤的评论（即使本校、其教职员、学生、承办商、住户、家长或供应商在网站或网志中没有明确点名，只要本校合理地相信他们是可识别的，雇员仍可能承担责任）。
- 对任何教职员发表任何可能构成非法歧视、骚扰或网络欺凌的评论，违反平等机会法例，或发布任何歧视性或可能构成非法骚扰或网络欺凌的图片或影片片段，教职员须为其根据该法例的行为承担个人责任。
- 披露属于本校、其教职员、学生、同事、承办商、住户、家长或供应商的任何商业秘密或机密、专有或敏感资料，或任何可能被本校的一个或多个竞争对手使用的资料，例如有关本校工作、产品和服务、技术发展、正在进行的交易或未来业务计划和员工士气的信息。
- 侵犯属于学院的版权或任何其他专有权益，例如未经许可使用他人的图像或书面内容，或在已获准复制特定作品的情况下未给予确认。 如员工希望在其网上个人档案上发布其同事或学生、承办商、居民、家长或供应商的图像、照片或影片，应先获得对方的明确许可。
- 教职员不应在互联网（包括社交网站）上发表任何可能被视为代表哈罗香港、不符合学院价值观和理念的个人意见或言论。

8.3 如果学校要求教职员删除任何令人反感的内容，他们必须立即删除。

8.4 员工应记住，即使他们已将账户隐私设置设置为限制访问或“仅限朋友”级别，社交媒体网站也是公开的论坛，因此他们不应假设他们在任何网站上的帖子将保持私密。

8.5 员工在使用社交媒体网站时也必须有安全意识，并应采取适当措施保护自己免受身份盗用，例如将他们的隐私设置置于高水平，并限制他们提供的个人资料数量，例如出生日期和地点。 此类信息可能构成其他网站（例如网络银行）上安全问题和/或密码的基础。

8.6 如果工作人员在网上发现有关学校的任何不准确信息，他们应首先向传播主管报告。

9. 病毒

9.1 所有外部文件和附件将使用扫描软件自动进行病毒检查。 互联网是计算机病毒的潜在宿主。 从互联网下载受感染的信息对学校计算机网络可能是致命的。 附加到传入电子邮件的文件可能嵌入了病毒。

9.2 如果工作人员担心电子邮件附件，或认为该附件没有自动扫描病毒，则应联系 ICT 部门，而无需打开附件或回复电子邮件。

10. 员工使用内部电子邮件的指引

10.1 学校在快节奏且有时压力很大的环境中运作，电子邮件被接受为日常使用的主要沟通方式之一。电子邮件可能是传达特定信息的最佳方式，但在数字信息「超载」的时代，所有员工都应该注意过度电子邮件驱动的文化的影响，并就与他人沟通的内容、时间和方式做出明智的选择。

10.2 随着许多人现在通过多个个人和工作设备访问电子邮件，以促进生产力和效率的方式适当使用电子邮件，同时使员工能够管理合理的工作与生活平衡变得越来越重要。

10.3 虽然寄件人有权随时发送电子邮件，但收件人也有权选择何时阅读收到的电子邮件，前提是这符合公认的专业行为水平，并符合对其角色和职责的期望。 不应普遍期望员工会阅读和回复深夜发送的电子邮件，但预计所有电子邮件都会在收到后 24-48 小时内（学期期间）得到某种形

式的回复——即使这只是一个等待回复。 如果在周末收到电子邮件，可能需要快速回复或发送保留回复，并在下一个上学日发送完整回复。

10.4 就目前被认为是良好做法而言：

- 应始终使用专业称呼和签字，例如亲爱的..... 然后是最美好的祝愿或亲切的问候。 如果两个人之间出现电子邮件线索，则可以删除问候。
- 在使用「全部回复」之前请三思而后行，确保正确使用抄送，并考虑电子邮件的所有参与者是否需要在初次交流后继续被抄送或包含在电子邮件追踪中。
- 考虑电子邮件的语气以及它可能传达的方式——请记住，来自不同文化和背景的人可能会有不同的解释。 因此，最好避免讽刺、幽默或口语化，并尽可能清晰地写作。
- 校对每封邮件，只有在电子邮件完成并检查完毕后才添加电子邮件地址。 这将防止任何电子邮件在编辑之前意外发送。
- 如果内容敏感，最好开会或打电话。 然而，如果必须发送敏感邮件，则应在发送前大声朗读讯息，以确保语气适当，避免误解。
- 当教职员离开学校或长时间无法工作时，应使用自动「不在办公室」通知。
- 没有什么是机密的 - 因此，请相应地写作并始终保持尊重，有尊严地对待他人。
- 学校的社会愿景：「一个充满关怀、尊重的社区，让每个人都茁壮成长」在我们的在线社区中同样重要。

11. 一般事项

11.1 本政策中描述的条款和建议行为并非详尽无遗，也不预期学校电子邮件和互联网设施的每一种可能使用。 我们鼓励员工谨慎行事，并考虑本政策的基本原则。

11.2 此原则可能会变更，目前版本会张贴在员工内部网络（SharePoint）上。

Dinesh Alwani，ICT 总监
2024 年 8 月

声明

本人认识到，当用户在线时，服务器会记录用户的行为，并且任何明显违反法律或学校规则的行为都可能受到调查。 本人同意严重违反电脑使用规则的行为将作为纪律事项处理，并在适用的情况下，警方或地方当局可能会参与其中。

学校保留权利，就任何教职员保管的电脑设备的任何损失或损坏，如未获保险索偿，收取任何自负额。

本人理解学校的社会愿景声明：“一个充满关怀、尊重的社区，让每个人都茁壮成长”，并同意在本人的所有在线活动中遵守这一声明。

本人已阅读并充分理解上述条件，并同意遵守：

签名

打印名称

科

日期

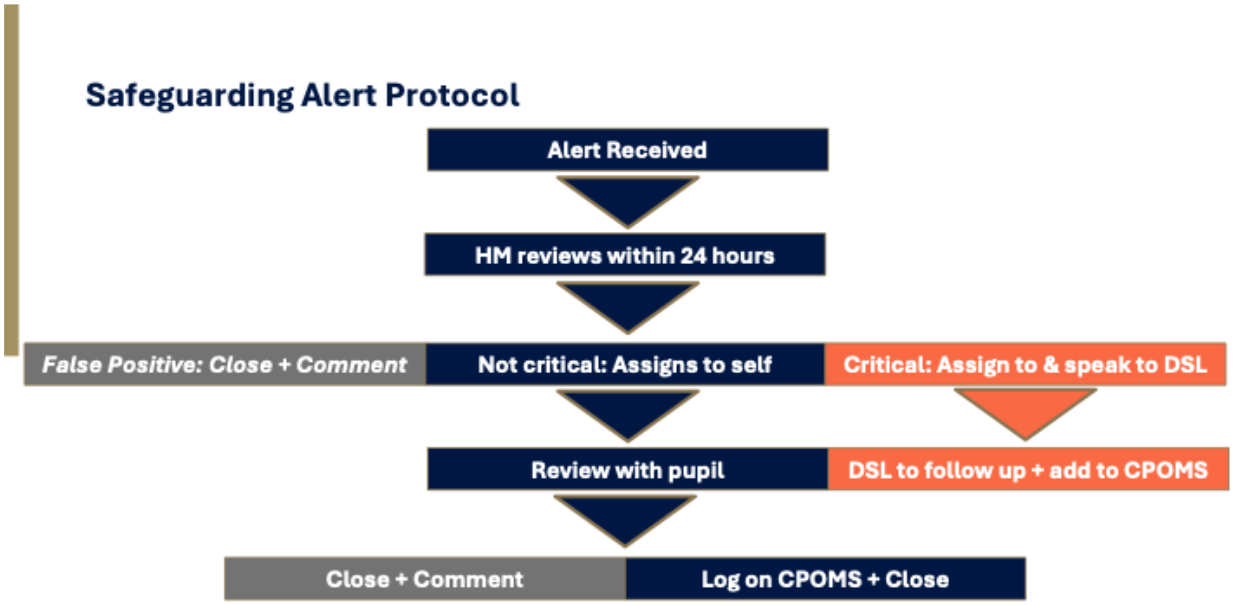
请签名并交回人力资源总监

E.A.海顿
校长

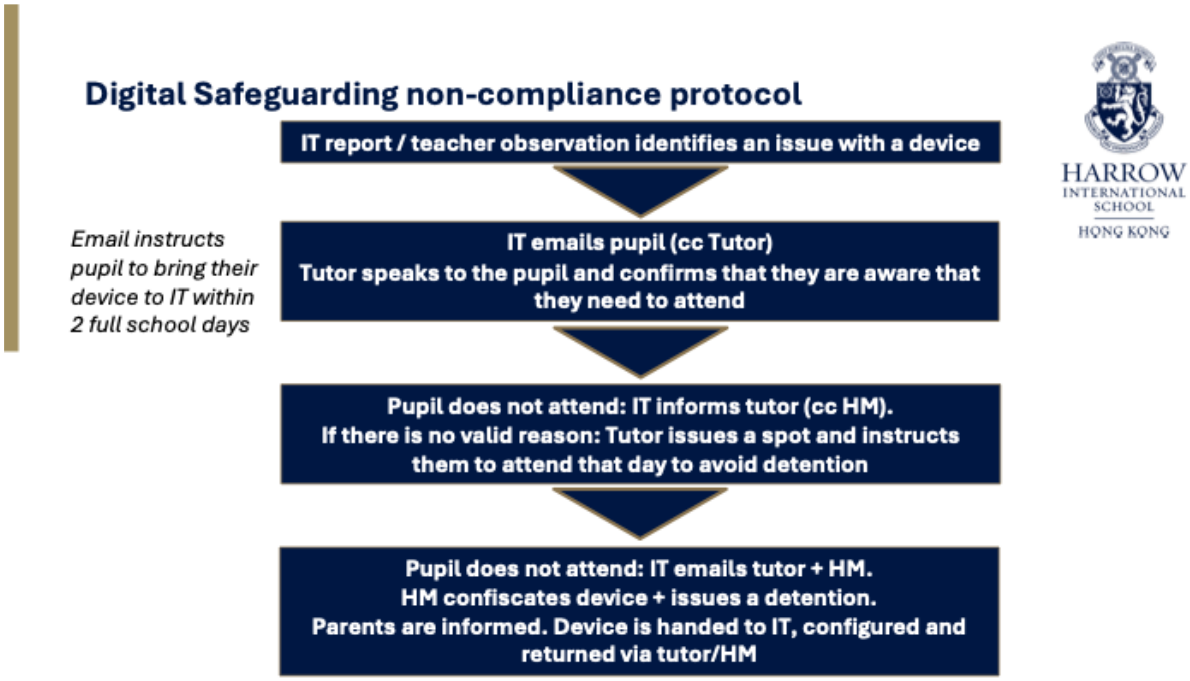
2024 年 8 月

评论日期：2024 年 7 月 31 日
下次评论：2025 年 8 月 1 日
所有者：信息通信技術總監

附錄 3：保障警示協議


Safeguarding Alert Protocol
Alert Received
HM reviews within 24 hours
False Positive: Close + Comment
Not critical: Assigns to self
Critical: Assign to & speak to DSL
Review with pupil
DSL to follow up + add to CPOMS
Close + Comment
Log on CPOMS + Close

附录 4：数字保护不合规协议



附录 5：数字安全回应协议

目的：

概述出现线上安全问题或事件时应采取的步骤。

响应步骤 ：

5. **报告：**
    a. 学生可以向老师、DSL 或其他值得信赖的成年人报告问题。
    b. 如果家长/监护人怀疑有问题，可以联系学校。
6. **调查：**
    a. DSL 将与 IT 和相关工作人员合作领导调查。
    b. 所有在线事件都会被记录下来以供将来参考。
7. **行动：**
    a. 根据严重程度采取纪律处分，从警告到设备限制。
    b. 为受网络欺凌或网络虐待影响的学生提供支持和咨询。
8. **跟进：**
    a. 与学生和家长进行跟进，以确保问题得到解决。

警戒 对过滤/监控问题的辅导响应的优先级 ：

优先事项 1 - 立即回应

- 自残/自杀相关内容
- 儿童保护/虐待材料
- 暴力的直接威胁
- 非法内容

优先事项 2 - 即日回应

- 网络欺凌事件
- 不当内容访问
- 多次尝试绕过安全性

优先级 3 - 48 小时响应

- 令人担忧的行为模式
- 多次尝试访问封锁的内容
- 不寻常的浏览模式

优先事项 4 - 每周回顾

- 违反一般政策
- 生产力问题
- 资源的非教育用途

附录 6：家长和监护人资源

目的：

为家长提供外部工具和资源，帮助确保孩子的上网安全。

主要资源：

- **联机安全信息：**
    - 英國更安全的互聯網中心： https://saferinternet.org.uk/
    - 常识媒体： https://www.commonsensemedia.org/
    - 互联网事务： https://www.internetmatters.org/
    - 家長資訊： https://www.educateagainsthate.com/resources/parent-info/
- **网络霸凌预防：**
    - StopBullying.gov： https://www.stopbullying.gov/
    - 国际儿童网： https://www.childnet.com/
    - 抛弃标签：： https://anti-bullyingalliance.org.uk/aba-our-work/our-members/core-members/ditch-label
    - Cybersmile 基金会： https://www.cybersmile.org/
- **家长监护和监控：**
    - 国家网络安全指南： https://nationalcollege.com/guides/what-parents-need-to-know-about-online-content-10-tips-to-keep-your-children-safe-online
    - OpenDNS： https://support.opendns.com/hc/en-us/articles/227988127-Getting-started-About-using-OpenDNS
    - Qustodio： https://www.qustodio.com/en/
    - 屏幕时间： https://support.apple.com/en-us/108806

附录 7：词汇表

目标：

定义政策中使用的技术和保护术语。

关键术语：

1. **学生安全：** 学生的安全和福祉。
2. **数字公民：** 学生负责任地使用技术，积极、安全地参与数字世界。
3. **正向数字文化：** 一种促进尊重、包容和负责任的线上行为的文化。
4. **数字风险：** 网络霸凌、隐私外泄和网络骚扰等网络危险。
5. **事件报告：** 报告和回应网络安全事件的程序。
6. **保障措施：**采取技术、教育和政策措施，保护学生免受线上风险。
7. **在线学习平台：** 用于在线学习活动的平台。
8. **个人设备：** 学生和教职员使用的笔记本电脑、平板电脑和其他设备。
9. **学校发放的设备：** 学校出于教育目的提供的设备。

附录 8：LightSpeed 过滤和自动警报时间表

小学部学生

时段	程序	过滤	监控	警报
在学校规则中	上午 7：00 - 下午 4：30	启用（LS 过滤器）	在	在
校外规则	下午 4：30 - 上午 6：59 及非上課日	启用（LS 过滤器）	关闭	关闭

初中部日间学生

时段	程序	过滤	监控	警报
在学校规则中	上午 7：00 - 下午 4：30	启用（ PS 过滤）	在	在
校外规则	下午 4：30 - 上午 6：59 及非上課日	启用（ OOS 过滤）	关闭	关闭

初中部寄宿生

时段	程序	过滤	监控	警报
在学校规则中	上午 7：00 - 下午 4：30	启用（ PS 过滤）	在	在
	下午 4 时 30 分至早上 6 时 59 分	启用（ OOS 过滤）	在	关闭
校外规则	非上课日	启用（ OOS 过滤）	关闭	关闭

9 年级走读生

时段	程序	过滤	监控	警报
在学校规则中	上午 7：00 - 下午 4：30	启用 （ Y9 过滤）	在	在
校外规则	下午 4：30 - 上午 6：59 及非上課日	启用（ OOS 过滤）	关闭	关闭

9 年级寄宿生

时段	程序	过滤	监控	警报
在学校规则中	上午 7：00 - 下午 4：30	启用 （ Y9 过滤）	在	在
	下午 4 时 30 分至早上 6 时 59 分	启用（ OOS 过滤）	在	关闭
校外规则	非上课日	启用（ OOS 过滤）	关闭	关闭

高中部走读生

时段	程序	过滤	监控	警报
在学校规则中	上午 7：00 - 下午 4：30	启用（SS 过滤）	在	在
校外规则	下午 4：30 - 上午 6：59 及非上課日	启用（ OOS 过滤）	关闭	关闭

高中部寄宿生

时段	程序	过滤	监控	警报
在学校规则中	上午 7：00 - 下午 4：30	启用（SS 过滤）	在	在
	下午 4 时 30 分至早上 6 时 59 分	启用（ OOS 过滤）	在	关闭
校外规则	非上课日	启用（ OOS 过滤）	关闭	关闭

附录 9：学生监察数据的资料保护及保存

1. **数据传输**

- 每周报告会以电子邮件中的SharePoint链接形式传送，因此不存在数据传输风险

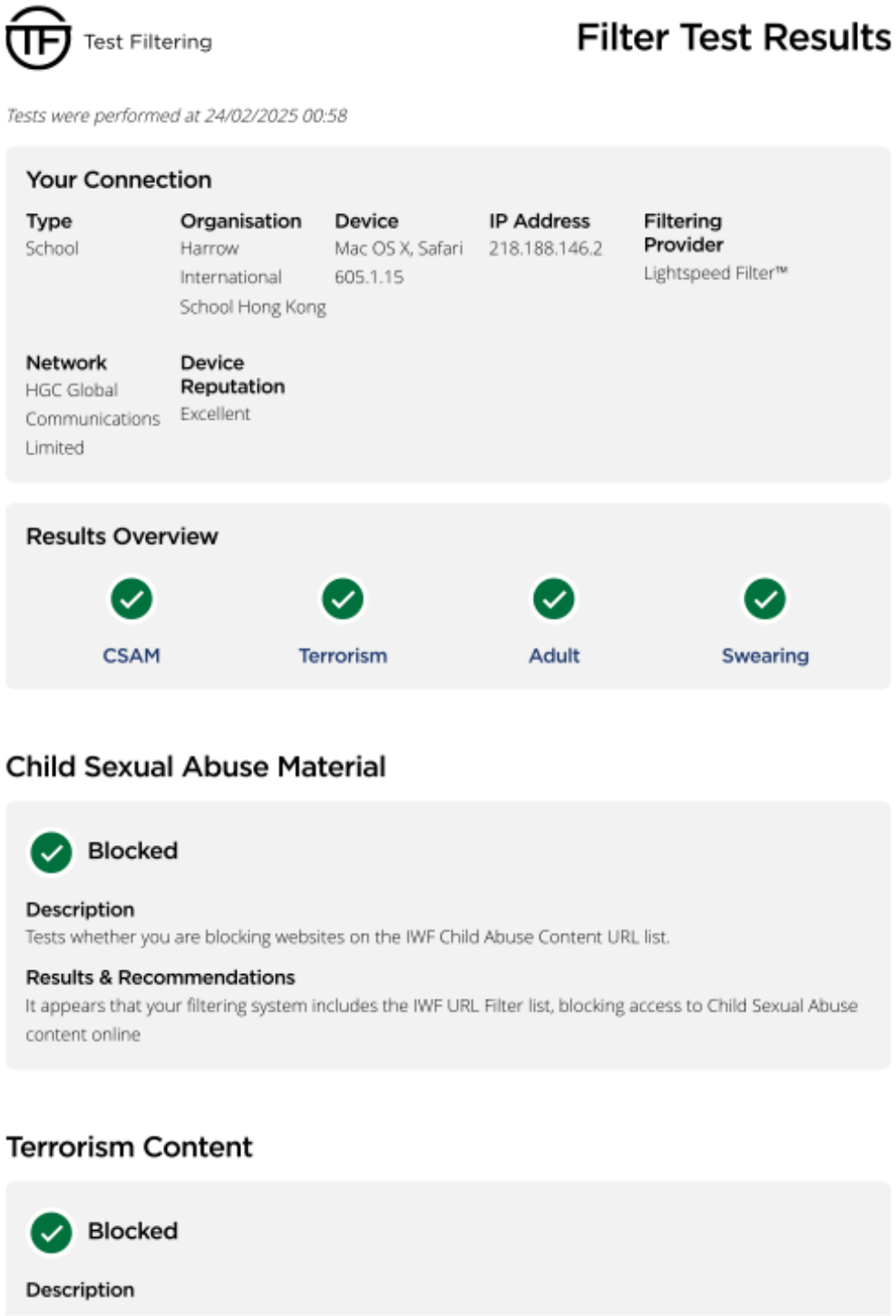
2. **资料储存**

- 地点：SharePoint [家庭辅导团队报告/文件/防火墙报告]
- 格式：加密数据库，具有对特定个人的访问控制
- 备份：SharePoint 数据透过 M365 自动备份

3. **资料保留期限**

- 网络活动记录：90 天
- 屏幕抓取：30 天
- 实时监测数据：60天
- 警报记录：90天
- 防火墙报告：90 天

附录 10：测试过滤结果


Test Filtering
Filter Test Results
Tests were performed at 24/02/2025 00:58
Your Connection
Type
School
Organisation
Harrow International School Hong Kong
Device
Mac OS X, Safari 605.1.15
IP Address
218.188.146.2
Filtering Provider
Lightspeed Filter™
Network
HGC Global Communications Limited
Device Reputation
Excellent
Results Overview
CSAM
Terrorism
Adult
Swearing
Child Sexual Abuse Material
Blocked
Description
Tests whether you are blocking websites on the IWF Child Abuse Content URL list.
Results & Recommendations
It appears that your filtering system includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online
Terrorism Content
Blocked
Description

Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

Results & Recommendations
It appears that your filtering system includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

Adult Content

Blocked

Description
Test whether your Internet filter blocks access to pornography websites

Results & Recommendations
It appears that your filtering system includes blocking for adult content. This indicates that your system has a list of adult websites or pages that are actively being blocked.

The test only checks to see if blocking is in place, and does not measure the effectiveness of the blocking across the range of available sources. Check with your filter provider that your system is setup in the most effective way, and matches your policy and needs.

Offensive Language

Blocked

Description
Accesses a page containing offensive language to test if your filtering software blocks it

Results & Recommendations
It appears that your filtering system includes blocking for offensive language