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.

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.
- 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.

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 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 further supported by physical monitoring by the house pastoral team, and IT tethering reports where required.

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**: Digital Safety Response Protocols
- **Appendix 4**: Resources for Parents and Guardians (e.g., links to websites on online safety)
- **Appendix 5**: Glossary of Terms
- **Appendix 6**: Lightspeed configuration settings
- **Appendix 7**: Data safeguarding and Retention
- **Appendix 8**: Test Filtering Results

Reviewed: February 2025
Next Review: August 2025
Owner: Assistant Head (Digital Strategy, Assessment and Tracking)
Version: 1

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

The School has a duty of care to ensure that each pupil at Harrow International School Hong Kong uses computer equipment and the Internet, as well as mobile phones and other electronic and communication devices responsibly. Pupils should expect their network and devices use 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. The School network is available for use by the whole School community, pupils should, therefore, use computer equipment and the Internet primarily for academic purposes and should not engage in any activity that may disrupt the effective operation of the network.

The code of conduct below applies to use of any machines connected to the School network, as well as personal computers or MacBooks, iPads, mobile phones and other electronic devices.

1. Pupils must never use another person's network account or allow their own network account to be used by another person; at all times, pupils are responsible for the security of their own password. A pupil concerned that others may know his/her password should either immediately change it or ask a member of the ICT Department to change it for him/her.
2. Pupils are forbidden from sending over the Internet or by any other means, any information, such as text or images, about the School or any individuals in it without permission.
3. Pupils must not attempt to access, send, display or store any offensive material (including images).
4. Any form of electronic communication (including email, the Internet or messaging systems) must comply with School rules, as well as generally accepted standards of language and behaviour; abusive language is unacceptable. The School's systems are able to intercept inappropriate electronic communication.
5. Pupils are not allowed to use Internet filter by-pass methods (VPN, Proxy severs, Anonymisers, etc.) or use any private wireless network independent of the School network (such as 5G networks)
6. Pupils are expected to use the printing facilities responsibly.

SANCTIONS

Any breach of the code of conduct will lead to sanctions (which involve loss of network account, loss of Internet access and email restricted to specified times) while the matter is being investigated. Offences with mobile phones or other electronic devices will lead to their confiscation. Normal School sanctions may then be applied depending on the severity of the offence, but pupils should be aware that the abuse of School and personal computer equipment, mobile phones or other electronic devices will be taken seriously. Misconduct during the holidays will be amenable to School discipline if the welfare of other people or the reputation of the School is placed at risk.

Dinesh Alwani, Director of ICT , September 2024

PUPIL ICT CODE OF CONDUCT (2024/25) [Lower School]

HARROW INTERNATIONAL SCHOOL HONG KONG

LOWER SCHOOL PUPIL DIGITAL CODE OF CONDUCT 2024-25

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: 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 4: 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 5: 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 6: 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 7: 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

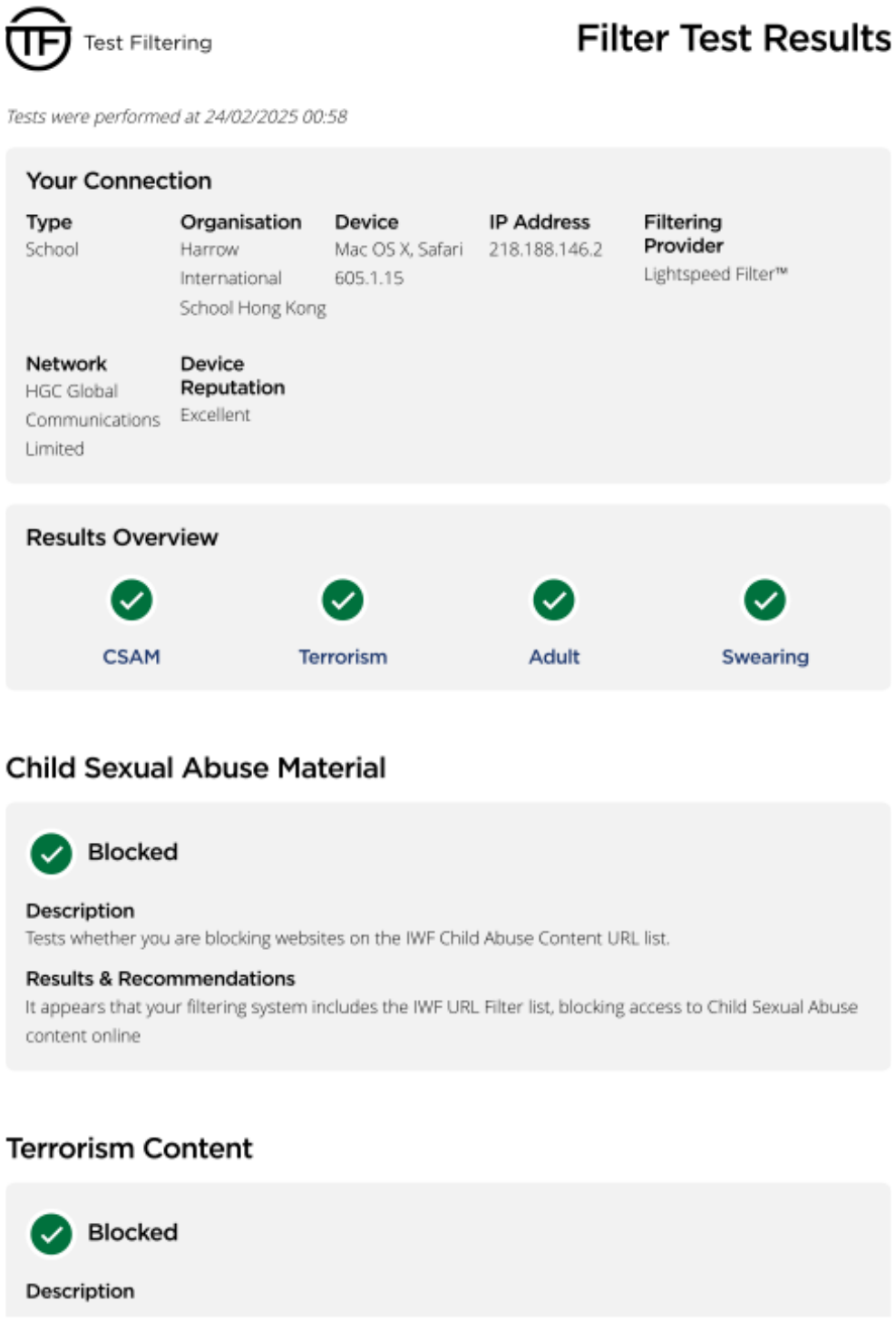
2. **Data Storage**

- 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 8: 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