



# Online Safety Policy

<b>1<sup>st</sup> version</b>	Nov, 2020
<b>2<sup>nd</sup> version</b>	Mar, 2021
<b>3<sup>rd</sup> Version</b>	April, 2022
<b>Next Review Date</b>	April,2023
<b>Monitoring will take place at regular intervals:</b>	Annually

## Table of Contents

Users must respect and protect the integrity, availability, and security of all electronic resources by: .....	8
Users must respect and practice the principles of community by: .....	8
Consequences for Violation .....	8
Supervision and Monitoring .....	8
Appendix .....	17
Flowchart for responding to e-safety incidents in school.....	17
Acceptable Use Agreement for students.....	18
.....	18
Staff Information Systems Consent Form .....	20
Information Confidentiality .....	21

### **Introduction:**

Internet and other digital information communication technologies are excellent tools that pave way to new opportunities in the world of education. Online safety plays an essential part in safeguarding children and young people in the digital age, especially in distance learning platform.

The Governors, staff, students and parents of **Harvest Private School** play a vital role in setting an example for the whole school and are central to implementing policy and process. It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This supports a robust online safety ethos and ensures that the school is providing the best online safety provision they possibly can.

Online safety is an omnipresent topic, which requires recurrent regulatory review and places a stringent duty of care on us all. This policy supports school in meeting statutory requirements as per the educational rules and regulations of MoE.

Our e-Safety Policy has been written by the school ICT has been agreed by the senior management team. The e-Safety Policy will be reviewed annually by ICT Leader, ICT Coordinator and senior member of staff.

### **Aim of Online Safety Policy:**

Harvest Private School ensures that:

1. Students can safely access new technology and learn how to participate in the digital world without compromising their safety and security.
2. A planned e-safety curriculum is provided and is regularly revisited.
3. Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
4. All students and staff understand the importance of password security and the need to log out of accounts.
5. Staff acts as good role models in their use of the Internet and mobile devices.
6. It has clear and understood arrangements for the security, storage and transfer of personal data.
7. To create awareness among the stakeholders on 'the various initiatives of U A E in relation to child protection.
8. It addresses subjects such as ICT security, invasion of privacy, malicious and illegal activities including hacking, fraud, improper system use, defamation, threats to state security, terrorism, insult to religions, and many more. etc.
9. It will deal with incidents within this policy and associated behavior and cyber bullying policies and will, where known, inform parents / caregivers of incidents of inappropriate e-safety behavior that take place out of school.

### **Links with other policies and practices:**

The online safety policy links with many other policies, practices and action:

1. Child Protection and Safeguarding Policy
2. Cyberbullying policy
3. Students Code of Conduct
4. Staff Code of Conduct
5. E- incidents Complaints procedure (refer to the appendix)
6. Password Policy
7. Data Protection Policy

## **Roles and responsibilities:**

### **Governors:**

The Governors have overall responsibility to monitor the policy, the School **Principal and Online safety Leader** accountable for implementation.

They will also co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the **online safety Leader**.

Governing Bod will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the School's ICT systems and the internet.

### **Principal and Senior Leaders:**

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Principal and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles

### **Online Safety Leader:**

- School's online safety leader set out schools' child protection and E-safety policy.
- Supporting the Principal ensuring that staff understands this policy and that it is being implemented consistently throughout the academic year.
- Working with the Principal, ICT coordinator and other staff, as necessary, to address any online safety issues or incidents.
- Ensure "An effective approach to online safety empowers a school to protect and educate the whole school in their use of technology and establishes mechanisms to identify intervene in and escalate any incident where appropriate."
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behavior policy.
- Updating and delivering staff training on online safety. All staff must read online safety policy and Acceptable use policy.
- Communicate with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Principal and Governors.
- Work with the Principal and Governors to ensure a framework for storing data, and ensure that child protection is always put first and data-protection processes support careful and legal sharing of information. Oversee and discuss 'appropriate filtering and monitoring' with Principal, Governors and local authorities and ensure staffs are aware.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the Principal and Governors.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends. Stay up to date with the latest trends in online safety.
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the community, with a strong focus

on parents. Communicate with school technical, pastoral, and support staff as appropriate.

- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure that staff adopt a zero-tolerance approach to sexual violence and harassment, as well as to cyber bullying.

### **ICT Coordinator**

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep student safe from potentially harmful and inappropriate content and contact online while at School, including extremist material.
- Ensuring that the School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School behavior policy.
- Keep up to date with the School's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the online safety leader / School systems and networks reflect policy
- Support and advice on the implementation of 'appropriate filtering and monitoring' to Principal and Governors.
- Maintain up-to-date documentation of the online security and technical procedures.

### **All HPS Employees**

- They have an up to date awareness of e-safety matters and of the current school / academy e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Head of Year for investigation / action / sanction
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### **Students**

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and

know how to do so

- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realize that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school or outside school if there are problems

### **Parents**

- School recognizes the crucial role that Parents play concerning the safety of our students. Parents are therefore encouraged to:
- Notify a member of Teaching/supervisors of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the School's IT systems and internet
- The School will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviors in their own use of technology,

### **Visitors and members of the community**

- Visitors and members of the community who use the School internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

## **E- Safe Education and curriculum**

### **Students**

- School recognizes that online safety and broader digital resilience must be embedding throughout the curriculum.
- The education of students in E-safety is an essential part of the school's E-safety provision.
- Students and young people need the help and support of the school to recognize and avoid e-safety risks and build their resilience.
- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum.
- It is the school E safety education team to identify opportunities to implement online safety through all school activities, both within the curriculum, or supporting curriculum and making the most of unexpected learning opportunities as they arise
- The E-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
  1. A planned e-safety curriculum should be provided as part lessons and should be regularly revisited
  2. Key e-safety messages should be reinforced as part of a planned programmed of assemblies and pastoral activities
  3. Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
  4. Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
  5. Students should be helped to understand the need for the students Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

### **Teaching Staff and Supervisors**

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- All staff should carefully supervise and guide students when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics that would normally result in internet searches being blocked. In such a situation, Teachers can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

### **Acceptable Usage Policy**

We in *Harvest Private School* are pleased to be able to offer our school community members access to computer technology, including access to the internet and educational platforms such as Microsoft office 365. We are dedicated to access and support of appropriate technology which unlocks our potential and connects us locally and globally.

All students, parents, staff, visitors, Governors are expected to sign an agreement regarding the acceptable usage policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the School's internet must be for educational purposes only, or for fulfilling the duties of an individual's role. **HPS** will monitor the websites visited by students, staff, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the **HPS acceptable usage policy and agreements**.

#### **Objective**

- Our students will be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.
- School computing systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school will ensure that students will have good access to computing to enhance their learning, and we expect the students and parents to agree to be responsible users.

We believe that the tremendous value of technology and the information technology network as an educational resource far outweighs the potential risks. We will leverage existing and emerging technology as a means to learn and thrive in the 21st Century and prepare our students for success toward their goals in the competitive global, electronic age. We feel that access to the tools and resources of a world-wide network and understanding when and how these tools are appropriately and effectively used are imperative in each student's education. If you have any doubt about whether a contemplated activity is acceptable, consult with your immediate teacher, supervisor, Principal to help decide if a use is appropriate.

## **Digital Devices**

A Digital Device is defined as an electronic device that can receive, store, process or send digital information. The following can be found in Harvest Private School:

- Smartphones/cellular phones
- Tablets
- iPads
- Laptop/notebook/ computers

May include other devices which can get internet access and store data

## **Users must respect and protect the privacy of others by:**

- Using only assigned accounts.
- Only viewing, using, or copying passwords, data, or networks to which they are authorized.
- Refraining from distributing private information about others or themselves.

## **Users must respect and protect the integrity, availability, and security of all electronic resources by:**

- Observing all school Internet filters and posted network security practices.
- Reporting security risks or violations to a teacher or network administrator.
- Not destroying or damaging data, networks, or other resources that do not belong to them, without clear permission of the owner.
- Conserving, protecting, and sharing these resources with other users.
- Notifying a staff member or administrator of computer or network malfunctions.

## **Users must respect and practice the principles of community by:**

- Communicating only in ways that are kind and respectful.
- Reporting threatening or discomfoting materials to a teacher or administrator.
- Not intentionally accessing, transmitting, copying, or creating material that violates the school's code of conduct or honor code (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).
- Not using the resources to further other acts that are criminal or violate the school's list of behavior.
- Avoiding spam, chain letters, or other mass unsolicited mailings.
- Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.

## **Consequences for Violation**

Violations of these rules may result in disciplinary action, including the loss of a user's privileges to use the school's information technology resources. Further discipline may be imposed in accordance with the school's Staff/students code of conduct and including suspension or expulsion depending on the degree and severity of the violation. For more details, refer to Staff Code of Conduct and Students Code of Conduct (which is "Student Behaviour Management Regarding Distance Learning 2020" taken from MOE).

## **Supervision and Monitoring**

The use of school owned information technology resources is secure, but not private. School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to

examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property.



They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

### ***Student's Role***

1. The school will monitor students' use of the computing systems and other digital communications on the school equipment.
2. Sharing of passwords, PINs, or other authentic information is strictly prohibited. Everyone is responsible for his/her account(s), including the safeguarding of access to the account(s).
3. The use of HPS resources, to access, further or otherwise participate in activity which is inconsistent with the mission of the school is prohibited. This includes, but is not limited to the following: illegal activity, hate speech, violent behavior & bullying, spam, hacking, etc.
4. The school computing systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
5. Students need to respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
6. Students should not take or distribute images or videos of anyone without their permission. Capturing screenshots of any online class or any member of online class including teachers or students and posting it elsewhere is considered offensive.
7. Students should immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online. Students will report any kind of safety issues or violations in any form to class teacher.
8. Students should not try to open any attachments to emails, unless I know and trust the person/organization who sent the email, due to the risk of the attachment containing viruses or other harmful programs/apps.

### ***Parents Role***

1. Keep the computer in a central place, where everyone can see what's on the screen.
2. Stay involved (without stepping on their toes constantly) on what students are doing online especially if it's got to do with searching and looking for new information etc.
3. Check out which sites they want to access, or which games they want to play and tell them if they are acceptable, until they reach a certain specified age.
4. Set time limits. Giving kids unlimited access to online causes unlimited problems for parents. Tell them how many hours they have a week.
5. Explain online habits. Explain strangers often play pretend games and they are not really who they claim to be.
6. Remind them the students that they should not engage in any form of cyberbullying – even as a prank. They should not do anything online that they would be ashamed of doing in real life.
7. Beyond online, watch what content you have on your computer. Often, we receive email that is not age appropriate for our children, but we leave that in our mailboxes or desktops.
8. If your children have started to do their homework online, or are gathering information, researching facts etc., explain to them clearly how they should not "copy and paste" (plagiarize) content for their homework, unless they mention sources etc. Their teachers should help them understand this, but you should make it clear that this is not on.
9. Be involved. Be alert. Show on-going interest in what they are playing, reading, doing online. And always remind them that there is life (and a wonderful one) outside that screen.

### **Staff Role**

1. Educate students on appropriate and acceptable use of devices.
2. Provide guidance to aid students in doing research and help assure student compliance of the acceptable use policy.
3. Monitoring of students' behavior when they are using devices.
4. Report any malpractices, issues, or threat found related to the students' use of devices.

### **Visitors' Role**

1. Visitors will be given highly restricted guest accounts which will not allow any access to personal data and that any misuse of the system

## **Electronic communications**

### **Email**

We use email systems across the school for staff and students .

- Email is the means of official electronic communication
- Appropriate behavior is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be considered as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the School into disrepute or compromise the professionalism of staff.
- Staff are allowed to use the email system for reasonable (not during lessons) use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behavior apply at all times.
- Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

### **School website**

The School website is a key public-facing information portal for the school communities with a key reputational value. The ICT department manages the site.

- The School Academic Departments have determined the information that must be available on a school website.
- Where other staff submit information for the website, they are asked to remember:
  1. Sources must always be credited and material only used with permission.
  2. Where student work, images or videos are published on the website, their identities are protected and full names are not published.

### **Cloud platforms**

Schools recognize the benefits of cloud platforms, to enhance teaching and learning. It is important to consider data protection before adopting a cloud platform or service – For online safety, basic rules of good password hygiene (“Treat your password like your toothbrush –never share it with anyone!”), expert administration and training can help to keep staff and students safe, and to avoid incidents. The OSL and ICT coordinator analyses and documents systems and procedures before they are implemented Cloud platforms, and regularly review them. The following principles apply:

- Privacy statements inform parents and children when and what sort of data is stored in the cloud
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that student’s data is not shared by mistake.
- Open access or widely shared folders are clearly marked as such
  1. Multi-factor authentication is used for access to staff or student data
  2. Student images/videos are only made public with parental permission
  3. Only School-approved platform (Microsoft Team) are used by students or staff to store student work

### **Digital images and video**

- Parents/carers are asked if they give approval for their child’s image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent). Parents answer as follows:
  1. For displays around the school
  2. For the newsletter, in school marketing
  3. For online website, For a specific high profile image for display
  4. For social media whenever a photo or video is taken/made.
  5. Any student shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them)

#### ***Refer to the Appendix***

### **Social media**

- Online Reputation Management (ORM) is about understanding and managing our digital footprint.
- Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. The appointed School ICT Members is responsible for managing individual schools Facebook account.
- However, as stated in the acceptable use policies which all members of the HPS community sign, we expect everybody to behave in a positive manner, engaging respectfully with the School and each other on social media, in the same way as they would face to face. This positive behavior can be summarized as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the School or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.
- Students are discouraged from ‘following’ staff, public/Private accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.
- Staff are reminded that they are obliged not to bring the School or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online.
- All members of the School community are reminded that particularly in the framework of social media, it is important to comply with the school’s policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

### **Appropriate filtering and monitoring**

- Keeping Children Safe in Education forces schools to “ensure appropriate filters and appropriate monitoring systems are in place and not be able to access harmful or inappropriate material.
- At the same time to be careful that “over blocking” does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.”
- Refer to ICT policy for more details.

### **Device usage**

Personal devices and bring your own device (BYOD) policy

- The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy.
- Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

### **Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject’s rights
- Secure
- Only transferred to others with adequate protection

The school must ensure that:

It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing from information risk incidents

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the ICT department

Staff must ensure that they:

At all times take care to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data

**Training & Awareness**

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalization.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).
- Each Online safety leader and coordinator will undertake child protection and safeguarding training, which will include online safety.
- They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Students will receive minimum 1-2 times awareness related to online safety topics

**Handling online-safety Complaints/suggestions/incidents**

It is energetic that all staff recognize that online-safety is a part of safeguarding. School procedures for dealing with online-safety will be connected with the following policies

- Child Protection Policy
- Cyber-Bullying Policy
- Behavior Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
  1. The School commits to take all reasonable precautions to ensure online safety, but recognizes that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on students when they come into school. All members of the School are encouraged to report issues to allow us to deal with them quickly and sensitively through the school’s escalation processes.
  2. Any suspected online risk or infringement should be reported to our complaint & suggestion system and the online safety leader.
  3. Any concern/allegation about School staff misuse is always referred directly to the Principal.
  4. The School will actively seek support from other agencies as needed (i.e. the local authority)
  5. We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or students engage in or are subject to behavior which we consider is particularly disturbing or breaks the law.

Refer to the appendix for handling procedure of online-safety Complaints/suggestions/incidents

## **Monitoring and standardization arrangements**

The school maintains Digital **safety logs** for behavior and safeguarding issues related to online safety. School has two types of monitoring, one is on school premises as physical monitoring & CCTV system, and the other is through Microsoft 365.

### **Cyber-bullying**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying,

- The School will ensure that students understand what it is and what to do if they become aware of it happening to them or others.
- The School will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- Teachers will discuss cyber-bullying with their students, and the issue will be addressed.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber bullying.
- In relation to a specific incident of cyber-bullying, the School will follow the processes set out in the School Behavior Policy. Where illegal, inappropriate or harmful material has been spread among students, the School will use all reasonable endeavors to ensure the incident is contained. The OSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### **Checking electronic devices**

School staff have the physical check as well as system check on Microsoft Teams to search for and, if necessary, delete inappropriate images or files on student' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the OSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence
- Report it to the police

Any searching of students will be carried out in line with the latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on student' electronic devices will be dealt with through the School complaints procedure.

### **School Respond to Misuse of school technology**

Where a student misuses the School's IT systems or internet, the School will follow the procedures set out in the Behaviour Policy.

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the School's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Employees code of conduct.

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The School will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

### **Social media incidents**

These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the School Behaviour Policy (for Students) or Code of Conduct. Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, The Schools will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline for support or help to accelerate this process.

### **Publishing Students' Images and Work**

- Photographs that include students will be selected carefully and will be published (based on parent acceptance)
- Students' names will be used anywhere on the Website or Blog in association with photographs (based on parent acceptance)

### **Information System Security**

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and updated regularly.

### **Protecting Data**

#### **School Data**

Backup is crucial for data protection. A regular data backup is done frequently to save our important files from inevitable data loss situations due to common events such as

- system crash
- malware infection
- hard drive corruption and failure

#### **Personal data**

Every teacher is going to have a school account on their personal laptop plus using school email address

#### **Assessing Risks**

- The school will take all reasonable protections to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is suitable and that the implementation of the e-safety policy is appropriate.

## **e-Safety Rules**

These e-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

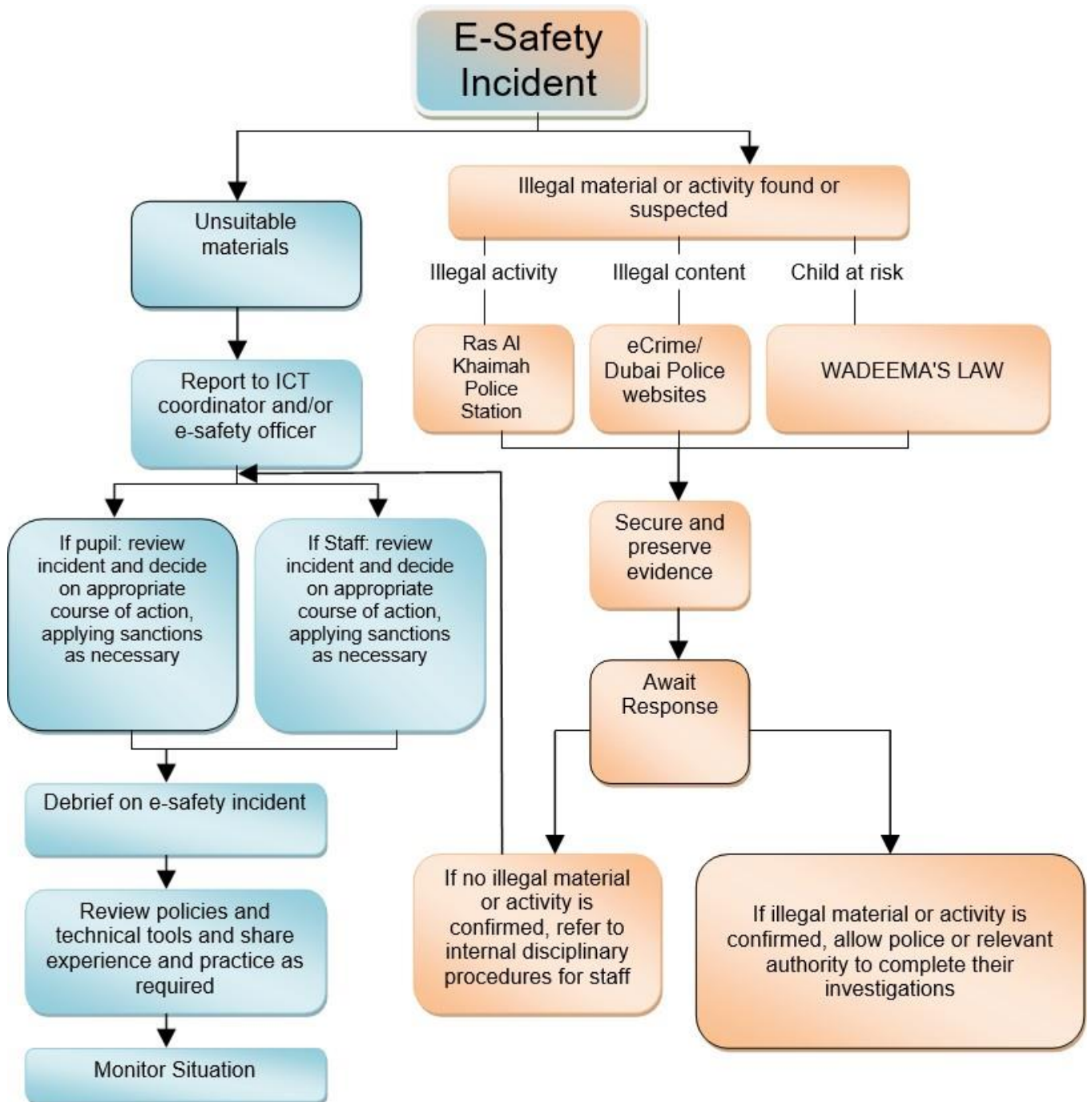
- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access (using the Firewall)
- Network access must be made via the user's authorized account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the headteacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorized use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorized or unlawful text, imagery or sound.



## Appendix

### Flowchart for responding to e-safety incidents in school



## Acceptable Use Agreement for students

<p><b>HARVEST PRIVATE SCHOOL</b> P.O.BOX 4328 Ras Al Khaimah , United Arab Emirates Email :harvestp.school@gmail.com</p> <p>e-Safe School المدرسة الآمنة رقمياً</p> <p>HPS HARVEST PRIVATE SCHOOL</p> <p>الجمهورية العربية المتحدة THE EMIRATES</p> <p>مدرسة هارفست الخاصة ص.ب 4328 رأس الخيمة. الإمارات العربية المتحدة</p> <p><i>Learner-based high-quality education</i></p>									
<h3>Acceptable Use Agreement for students – e-safe School</h3> <h3>اتفاقية الاستخدام المقبول لطلاب – المدرسة الآمنة رقمياً</h3>									
<ul style="list-style-type: none"> <li>I will take care and use HPS IT equipment properly.</li> <li>I will only share my user's name and password with trusted adults.</li> <li>I will tell an adult if I see anything that upsets me.</li> <li>I will be responsible and polite when I use the internet.</li> <li>I will use a safe name and not my real name on the internet.</li> <li>I know that I am allowed to use the internet only if my teacher gives me a permission.</li> <li>I will only take a photo or video of someone if they accept it.</li> <li>I am going to send only polite/kind messages.</li> <li>I will not intentionally write anything may upset other people.</li> <li>I do understand that the school may contact my parent/carer if I don't use school IT equipment properly.</li> <li>I do understand that if I don't follow these rules, I may not be allowed to use my school's account, devices or internet for a while, even if it was done outside school premises</li> </ul>	<ul style="list-style-type: none"> <li>سأحرص عند استخدام معدات التقنية الخاصة بالمدرسة واستخدامها بشكل صحيح.</li> <li>سأشارك اسم المستخدم وكلمة المرور الخاصة بي فقط مع البالغين والموثوق بهم.</li> <li>سأخبر شخصاً بالغاً إذا رأيت أي شيء يزعجني.</li> <li>سأحرص على أن أكون مسؤولاً ومهذباً عندما أستخدم الإنترنت.</li> <li>سأستخدم اسماً آمناً وليس اسمي الحقيقي على الإنترنت.</li> <li>أعلم أنه لا يُسمح لي بالدخول إلى الإنترنت إلا إذا سمح لي معلمي بذلك.</li> <li>لن ألتقط صورة أو مقطع فيديو لأ شخص إلا إذا سمح لي بذلك.</li> <li>سوف أرسل فقط رسائل مهذبة و لطيفة.</li> <li>لن أكتب عمداً أي شيء يزعج الآخرين.</li> <li>أفهم أن المدرسة قد تتحدث إلى أحد والدي أو مقدم الرعاية إذا كانوا قلقين بشأن استخدامي لمعدات التقنية الخاصة بالمدرسة.</li> <li>أفهم أنه إذا لم أتبع هذه القواعد ، فقد لا يُسمح لي باستخدام حساب المدرسة الخاص بي أو أجهزة أو انترنت المدرسة لفترة من الوقت ، حتى لو تم ذلك خارج المدرسة.</li> </ul>								
<p>The Acceptable Use Agreement has been discussed with a student who agrees to follow the e-Safety rules and to support the safe use of ICT at Harvest Private School, Ras AL Khaimah.</p> <p>تمت مناقشة اتفاقية الاستخدام المقبول مع الطالب الذي وافق على اتباع قواعد السلامة الإلكترونية ودعم الاستخدام الآمن لتكنولوجيا المعلومات والاتصالات في مدرسة هارفست الخاصة ، رأس الخيمة</p>									
<table border="1"> <tr> <th>Student's Name - اسم الطالب</th> <th>Class/section – الصف و الشعبة</th> </tr> <tr> <td>.....</td> <td>.....</td> </tr> <tr> <th>Parent's/carer's name - اسم ولي الأمر / مقدم الرعاية</th> <th>Parent's/carer's signature - توقيع ولي الأمر / مقدم الرعاية</th> </tr> <tr> <td>.....</td> <td>.....</td> </tr> </table>	Student's Name - اسم الطالب	Class/section – الصف و الشعبة	.....	.....	Parent's/carer's name - اسم ولي الأمر / مقدم الرعاية	Parent's/carer's signature - توقيع ولي الأمر / مقدم الرعاية	.....	.....	
Student's Name - اسم الطالب	Class/section – الصف و الشعبة								
.....	.....								
Parent's/carer's name - اسم ولي الأمر / مقدم الرعاية	Parent's/carer's signature - توقيع ولي الأمر / مقدم الرعاية								
.....	.....								
<p>Cambridge Assessment International Education Cambridge International School</p>									

## Acceptable Use Agreement for Staff

### Acceptable Use of Agreement Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

*IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents.*

- I will only use the school's email /internet /Learning Platform and any related technologies for professional purposes.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not use or install any hardware or software without permission from the ICT department.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken with school devices, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head of section.
- I understand I cannot use my mobile phone to take photos of children
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head of section.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

*I agree to follow this code of conduct and to support the safe use of ICT throughout the school*


*Signature ..... Date .....*

*Full Name .....*

*Job title: .....*

# Staff Information Systems Consent Form

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

		<b>Harvest Private School</b>	
<b>Employee E-Safety Consent Form</b>			
<b>Employee Information</b>			
Employee Name:		Date:	
Employee ID:		Job Title:	
		Department:	
<b>School E-Safety Processes</b>			
<input checked="" type="checkbox"/> School User Account	<input checked="" type="checkbox"/> School Official E-mail	<input checked="" type="checkbox"/> End User Antivirus	
<input type="checkbox"/> No Personal Account	<input type="checkbox"/> No Personal E-mail	<input type="checkbox"/> No USB Drive without Permission	
<input type="checkbox"/> Information confidentiality	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>			
<b>Details</b>			
I am _____ and I'm working in Harvest Private School as _____			
<b>Acknowledgment of Receipt of Warnings</b>			
By signing this form, you confirm that you understand the information in this form. You also confirm that you have discussed the form and a plan for improvement. Signing this form necessarily indicates that you agree with this form.			
Teacher / Staff member Signature		Date	
Principal Signature		Date	

Information Confidentiality

Harvest Private School  
RAK, UAE  
Email: harvestp.school@gmail.com  
Day\Date:

مدرسة هارفست الخاصة  
رأس الخيمة

Learnner-based high-quality education

Dear Staff:

During your employment at Harvest Private School, you may have access to confidential and proprietary data, which is not known by competitors, students, parents and staff. This information (hereinafter referred to as "Confidential Information") includes, sensitive details concerning the structure, conditions, and extent of their existing services and personal information, This Confidential Information is a valuable asset of the school, and it's NOT allowed to be shared!

Department: \_\_\_\_\_

**School E-Safety Processes**

<input checked="" type="checkbox"/> School User Account	<input checked="" type="checkbox"/> School Official E-mail	<input checked="" type="checkbox"/> End User Antivirus
<input type="checkbox"/> No Personal Account	<input type="checkbox"/> No Personal E-mail	<input type="checkbox"/> No USB Drive without Permission
<input checked="" type="checkbox"/> Information confidentiality	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		

I am \_\_\_\_\_ and I'm working in Harvest Private School as \_\_\_\_\_

Received and Agreed

Signature: \_\_\_\_\_

E- Safety Team

## Student Media Consent and Release Form

Harvest Private School  
RAK. UAE  
Email :harvestp.school@gmail.com



مدرسة هارفست الخاصة  
رأس الخيمة

*Learner-based high-quality education*

### Student Media Consent and Release Form

*Throughout the school year, students may be highlighted in efforts to promote HPS activities and achievements. For example, students may be featured in materials to train teachers, school social media and/or increase public awareness of our school through newsletter, yearbook, website, DVDs, displays, brochures, and other types of media.*

I, as the parent or guardian of \_\_\_\_\_, hereby give HPS and its employees, representatives, and authorized media organizations permission to use, print, photograph, and record my child for use in audio, video, film, or any other electronic, digital and printed media.

- a. This is with the understanding that neither HPS nor its representatives will reproduce said photograph, interview, or likeness for any commercial value or receive monetary gain for use of any reproduction/broadcast of said photograph or likeness. I am also fully aware that I will not receive monetary compensation for my child's participation.
- b. I further release and relieve HPS, its governors, employees, and other representatives from any liabilities, known or unknown, arising out of the use of this material.

I certify that I have read the Media Consent and Release Liability statement and fully understand its terms and conditions.

Name of child \_\_\_\_\_ Grade \_\_\_\_\_

Signature of parent or guardian \_\_\_\_\_

Date \_\_\_\_\_ Phone Number \_\_\_\_\_