ONLINE SAFETY POLICY

AY: 2025 - 2026

Date of Policy	August 2021
Date of last review	August 2025
Date of next review	August 2026
Lead Member of Staff	Principal & Head of Wellbeing

Online Safety Policy (2025 - 2026)

Introduction

The spirit of Vernus International School strives to reinforce a wide range of resources including web-based and mobile learning. It is also important to recognize the constant and fast-paced evolution of ICT within our society particularly where students are using internet technologies in virtual learning. While working in classrooms, students use:

- Websites, Learning Platforms (MLE) and Virtual Learning Environments
- Email, Instant Messaging, Chat Rooms, Social Networking & Blogs
- Podcasting & Video Broadcasting, Downloading from the Internet & Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Related Policies that Are Required of Schools

- Wellbeing Policy
- Social Media Policy
- Acceptable Use Policy

Purpose of Policy

The purpose of this policy is to ensure that all students and staff enjoy a safe online working environment free from any online security & safety issues. This policy serves the entire school.

Aims and Objectives

- To understand the responsibility to educate our students in e-safety issues;
- To teach them appropriate behaviors and critical thinking to enable them to remain safe and legal when using the internet and related technologies, in and beyond the classroom's context.

E-Safety & Security – Whole School Approach

All members of the school community have a responsibility for promoting and supporting safe behaviors in their online activities and follow school e-safety procedures. The ICT & ESafety leaders will ensure they are up to date with current guidance and issues through organizations such as Child Exploitation and Online Protection. They then ensure that the Section Heads, Head of Wellbeing & SLT are also updated, as necessary. All staff should be familiar with the school's policy including:

- Safe use of e-mail, internet, school network, equipment, and data

- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
  Publication of student information/photographs on the school website & social media
- Procedures in the event of misuse of technology by any member of the school community
- Their role in providing e-safety education to students.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Principal and SLT

- The principal has a duty of care to ensure the online safety of members of the school community
- The principal and head of wellbeing should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of the school
- The principal and Senior Leaders are responsible for ensuring that the head of wellbeing 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 to provide a safety net and support to those colleagues who take on important monitoring roles

Head of Wellbeing:

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the school technical staff and or KHDA/ relevant body whenever required

- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with the E-Safety Governor to discuss current issues, review incident logs, and filter/change control logs
- Attends relevant meetings/committees of Governors & Reports regularly to the Senior Leadership Team

IT/Technical staff:

The ICT/Computing staff is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- The use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal, SLT, Head of Wellbeing
- The filtering policy (if it has one), is applied and updated on a regular basis, and that its implementation is not the sole responsibility of any single person
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are constantly changed
- That the school meets required e-safety technical requirements and any KHDA/other relevant body E-Safety Policy/Guidance that may apply.
- They keep up to date with e-safety technical information to effectively carry out their safety role and to inform and update others as relevant

Teaching and Support Staff

Are responsible for ensuring that:

- All digital communications with students/parents/guardians should be on a professional level and only carried out using official school systems
- In lessons where internet research is pre-planned 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
- 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
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding this device

○

- They have an up-to-date awareness of e-safety matters and the current school esafety policy and practices and they have read, understood, and signed the Staff Acceptable Use Policy/Agreement (AUP). They report any suspected misuse or problem to the Head of Wellbeing/Section Head for investigation/action

Child Protection / Safeguarding Designated Safeguarding Lead

CPO (Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

Sharing of personal data ○ Access to illegal/inappropriate materials ○ Inappropriate online contact with adults/strangers ○ Potential or actual incidents of grooming ○ Cyber-bullying

Parents/Guardians

- Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices/Laptops/iPads in an appropriate way.
- The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, websites, and information about national/local e-safety campaigns/literature.
- Parents and caregivers will be encouraged to support the school in promoting good safety practices and to follow guidelines on the appropriate use of:
- ○ Digital and video images taken at school events
- ○ Their children's devices in the school (where this is allowed)

Students:

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

- Should understand the importance of adopting good e-safety practices 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 in the school.

Whole School Approach

E-mail

The use of email within the school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff-based or student-based, within school, between schools, or internationally. We recognize that students need to understand how to style an email in relation to their age.

- Under no circumstances should staff contact students or parents using personal email addresses.
- Students may only use school approved accounts and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school. Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- All students must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff must inform a member of SLT if they receive an offensive e-mail.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening, or bullying in nature and must not respond to any such communication
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of the staff

Education

○

Education – Students

The education of students in e-safety is an essential part of the school's e-safety provision. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned program of assemblies and pastoral activities
- 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
- Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the Internet, and mobile devices
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

Education – Parents / Guardians

Many parents have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviors. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and caregivers through:

- Letters, newsletters, website

- Curriculum activities
- Parents / Caregivers evenings/sessions
- Reference to the relevant websites and/or publications

Education – The Wider Community

The school will provide opportunities for local community groups to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- The school website will provide e-safety information for the wider community ○ E-safety messages targeted toward grandparents and other relatives as well as parents
- Providing family learning material in the use of new digital technologies, digital literacy, and e-safety

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows

- A program of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All fresh staff should receive e-safety training as part of their induction program, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements
- Head of Wellbeing will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organizations
- Head of Wellbeing will provide advice, guidance, or training to individuals as required.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings

Training – Governors

- Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee involved in technology, e-safety health and safety, or child protection. This may be offered in several ways:
- Participation in school training/information sessions for staff
- Attendance at training provided by the KHDA or other relevant organization

Strategies of Acceptable Use Guidance

Technical Infrastructure - Equipment, Filtering and Monitoring

VIS IT & Operations department will be responsible for ensuring that the school infrastructure/network is as safe and secure as possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that IT staff will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems, and cabling must be securely located, and physical access restricted
- All users will have clearly defined access rights to school/academy technical systems and devices

- The Operations Manager & IT staff are responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use
- Agreement ○ An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts that might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software
- An agreed policy is in place for the provision of temporary access of "guests"
- (interviewees, presenters, visitors) onto the school systems)

Bring Your Device (BYOD)

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 technologies to provide greater freedom of choice and usability. However, there are a few e-safety considerations for BYOD that need to be acknowledged by students & staff:

- The school has a set of clear expectations and responsibilities for all users
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, or change of ownership of the device will be reported as in the

- BYOD policy Any user leaving the school will follow the process outlined within the BYOD policy

Publishing student's images and work

- On a child's entry to the school, all parents/guardians will be asked to permit for their child's photo to be taken and to use their child's work/photos in the following ways on the school website
- Display material that may be used in the school's communal areas
- Display material that is used in external areas, i.e. exhibition promoting the school General media appearances, e.g. local/ national media/ press releases sent to the press
- highlighting an activity (sent using traditional methods or electronically. Students' names/full names will not be published alongside their image and vice versa without the Parent's consent.

Social networking and personal publishing

We block/filter access for students to social networking sites such as Facebook, TikTok, Snapchat Instagram, etc. in school. Students and parents will be advised that the use of social network spaces at home is inappropriate for primary-aged students. Students will be advised never to give out personal details of any kind that may identify them or their location.

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 for limited purposes
- Adequate, relevant, and not excessive
- Accurate secure & kept no longer than is necessary
- Processed & transferred by the data subject's rights & adequate protection

The school must ensure that:

- It will hold the minimum personal data necessary to perform its function and not for the purposes it was collected.
- It has a Data Protection Policy & it has clear and understood arrangements for the security, storage, and transfer of personal data

- There are clear and understood policies, clear Data Protection clauses, routines for the deletion and disposal of data in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud/Google Drive which ensure that such data storage meets the requirements laid down by the Operations department.

Staff must ensure that they:

- Always take care to ensure the safe keeping of personal data, minimizing its loss or misuse. v 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
- Transfer data using encryption and secure password-protected devices

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

- Video recording is not allowed by students during lessons. The sending of abusive or inappropriate text messages is forbidden.
- All classes have been issued Microsoft Teams that they can use for communication & learning purposes.

Responding to e-safety incidents/complaints

As a school, we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies, and the speed of change, it is not possible to guarantee that unsuitable material will never appear. The school cannot accept liability for material accessed, or any consequences of Internet access. Complaints relating to e-safety should be made to the head of wellbeing or a member of the senior leadership team.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offense;
- Investigation by the principal, head of wellbeing & section head, immediate suspension, leading to dismissal and involvement of police for serious offenses.
- Students and parents will be informed of the complaint's procedure.
  Parents and students will need to work in partnership with staff to resolve issues.

Reporting

As a school, we encourage victims and witnesses to speak up. Staff will be alert to changes in behavior, attitude, and well-being. All incidents will be treated seriously, however trivial they might seem at first. Every individual in school must report an incident of online safety issue whether it happens to themselves or another person.

Communication

The school communicates with parents on any incidents and investigations. We work in partnership with parents and students to prevent any E-Safety issues and to deal with any incidents of online safety issues.

Disciplinary Structures to Deal with Online Safety Issues

In line with the KHDA, the VIS Online Safety procedures & UAE government E-safety law and regulations, the online safety cases are of high-level violations.

Accordingly, the school applies the following behavior modification methods.

Sr. No.	Violation Level	Violation Decision
1	1st Violation	• 1/2 day internal exclusion • Warning Form no 1 & 2 • Parents are notified (written and verbal)
2	2nd Violation	• 1 -2 Day exclusion • Warning Form no 3 & 4 • Parents are notified (written and verbal) • Meeting with parents
3	3rd Violation	• 3 -5 days exclusion • Warning Form No. 5 - 7 • Parents are notified (written and verbal) • Meeting with parents • Re-registration Reviewed

Review

This policy will be reviewed at least once a year by the principal and the head of wellbeing.