



Draft: Positive Behaviour  
in the Digital Environment  
with a focus on Online Safety  
2015

**21st Century Competencies**  
Helping Digital Literacy

Department of eLearning  
From Enhancement to Transformation

# Contents

Page	
3	<b>Introduction</b>
3	<b>Policy principles</b>
3	<b>Managing and monitoring</b>
3	The development of the policy
3	Authorised access
4	Filtering and monitoring
5	Risk evaluation
5	<b>Teaching and learning</b>
5	The curriculum
6	Enhancing teaching and learning
7	Content evaluation
7	<b>Communication and content</b>
7	Site content
8	Virtual platforms
8	Use of email
9	Communication and social media
11	Mobile devices (including BYOD)
12	Video conferencing
13	Cyberbullying
13	Data protection
14	<b>Implementation</b>
14	Policy practice – students
14	Policy practice - teachers
15	Policy practice – parents
15	Handling complaints

## Introduction

The scope of this policy is to ensure that, all stakeholders in schools get a clear picture of what the use of the Internet entails and be informed of its proper use. Thanks to this policy, it is hoped that users of the Internet do so responsibly, minimising risks and avoid breaking any laws in the process. Staff in schools or in contact with pupils<sup>1</sup> are urged, to familiarise themselves with this policy as well as related documents such as the Code of Ethics for the teaching profession and the Acceptable Use Policy. The latter may be found on the Fronter platform.

The Ministry for Education and Employment wholly believes in digital literacy and its effective use in teaching and learning. It considers secure access Internet as a right to students. Actually, it has at heart this secure access, across all teaching grades<sup>2</sup> using Internet as a teaching tool or resource, at any given time of the day. In view of this, MEDE is structuring a policy towards good practices in an online environment, outlining the basics and garnering feedback from schools. Concurrently, schools will be given a level of autonomy to frame their own rules regarding online security.

## Policy Principles

The main principles of the policy will be as follows:

- All users are to be given access to educational resources.
- Protection to all users will be offered against indecent online material, cyberbullying and other forms of online harassment.
- All users will be fully informed as how to access and utilise online material responsibly and in a professional manner.

## 1 Managing & Monitoring

### 1.1 The Development of the Policy



The policy regarding proper use of online material will be integrated into the revisionary process within education, as per the Development Plan for Schools. This policy will also relate to other standing policies such as those for behaviour, anti-bullying and homework.

The policy will be drawn up by the school, modelled on a pre-existing structure which has been set up by the Department of eLearning. It will get approval both from the administration and the College Principal and it will be revised and updated on a yearly basis.

### 1.2 Authorised Access

Internet access to students will be deemed as their right and considered part of their educational needs, just as much as it is for teachers, to have wider availability to educational resources. Parental<sup>3</sup> permission to grant access to Internet will be required, during the students' first year and again at their fourth year in the education system.

- MITA will act as a service provider in schools. This is necessary to be able to monitor lines and maintain them. Furthermore, any potential, unauthorised access can be detected and reported to the authorities.
- In case where schools use other ISPs, these service providers will be bound to monitor any misuse or attacks and issue reports. Should there be any, the schools are to immediately inform MEDE (this point can be ignored if the school's sole ISP is MITA).
- As a matter of precaution, schools will keep records of staff and students who have access to Internet. These records are to be updated regularly and any irregularities noted (such as instances where students have their access privilege, withheld).
- An agreement between Primary and Middle schools and the students' parents/guardians should be in place, whereby, the policy regarding proper use of online material is, made explicitly clear to both parties. This agreement will also include a guide to what audio visual material can be uploaded online and the risks involved.
- Secondary students will be asked to sign and abide by the policy for proper use of Internet. The parents/guardians will be asked to put their signature as well (see eSafety Program).
- During the students' first and second years in school, Internet access will be under supervision by an adult. Access will be allowed only for specific, educational material which would have preferably been, properly researched beforehand and approved, whenever possible.
- Parents/Guardians will be duly informed that their children will be given supervised access to Internet. A sample letter will be endorsed with a copy of the eSafety Program.

### 1.3 Filtering & Monitoring



Despite one's best efforts at setting up a top notch filtering system, nothing is foolproof or stays such for a long time, when dealing with online hazards. To eliminate all risks, one would have to unrealistically, deny all access to the Internet. In a digital world, that would be counter-productive. Therefore, a balance must be struck between making the best out of online resources and keeping risks to the lowest level possible. Different levels of accessibility and supervision will be applicable to students according to their age and their familiarity with the Internet. This way, it is hoped, students are not put off by too many restrictions to their online access whilst at the same time, exposure to risks is kept under control.

- All staff will have the highest privileges to access online material, within the school filtering software.
- MITA and MEDE will still keep an eye on online activity and will from time-to-time, update their lists of prohibited online material and off-limits websites.
- MEDE will implement any feedback from the schools to bolster the protection to students, by keeping their filtering structures, updated and maintained.

- If and when, students or teachers come across websites which are of a dubious or indecent nature, the URL should be communicated to the MEDE.
- Both MEDE and the school's management will collaborate to regularly check that the filtering system is effective yet, not too extreme.
- Any suspicious online material or that which might put users at risk, schools might come across, must be escalated to the authorities such as the school's management, MEDE, Appogg or the Police, accordingly.

## 1.4 Risk Evaluation



The quantity of information to be found on the web has become staggering and so much widespread. This information is expanding by the second therefore it would be an impossible task to try to filter each and every bit of it. MEDE can and will impose filters on online material, however, experience has shown that being over-precautious, would render online searches useless to teachers. Eliminating all the risks would mean having to impose so many restrictions, that access to the Internet would become impractical.

- Like other forms of media such as magazines, books and videos, the Internet is also rife with information which is not appropriate to students. As previously declared, MEDE will do its utmost to partition this information from the students' reach, however, given the nature of the Internet, it cannot guarantee, that occasionally, undesired information, will not make it through the filters and into the students' computers and tablets. Should this unfortunately happen, neither MEDE nor the school concerned can be held responsible for this occurrence or any consequences it might bring about.
- Risk evaluation will be an ongoing exercise and methodologies will be applied to identify, evaluate and curb the risks involved.
- The school administration has to make sure that all users are aware and that they stick to the policy of proper use of online material.
- Unauthorised access to the Internet and misuse of computers to access prohibited online material may constitute a criminal act. (see Chapter 9: Subtitle V: Of Computer Misuse: pg.144ff)

## 2 Teaching & Learning

### 2.1 The Curriculum

The Internet has become an integral part of teaching and learning, so much so that the curriculum requires students to make competent and responsible use of it. Teachers need also to keep their pace by integrating the use of technology into their teaching. Digital competence is a requirement which is becoming fundamental for employability and life-long learning. Actually, digital literacy has become one of the tenets of education.

- The use of Internet is considered part of the curriculum and an implement to be used by both students and teachers.
- Use of Internet in schools will target a number of objectives, mainly, increasing the quality standard of education, improving results obtained in other areas of education besides information technology, contributing towards a better professional portfolio of teachers and finally, making life easier whether being at an office or administering a school.
- Whilst Internet access will be considered a right, breaching or misusing it, will have repercussions such as its suspension.
- Internet has become a staple ingredient in life, education, business and social interaction, therefore, MEDE will strive to provide suitable Internet access to students and teachers alike.
- Outside school hours, students will definitely have access to un-filtered Internet. Keeping this in mind, it is imperative that they are made aware of its pitfalls and how they can avoid them. They will also learn to evaluate the information they'll come across and distinguish whether it is suitable for them or not.

## 2.2 Enhancing teaching & learning



The benefits of Internet access in education incorporate the following:

- Worldwide access to resources related to education.
- Local access to resources as per above.
- Sharing of ideas and resources between students across countries in Europe, thanks to learning platforms such as eTwinning.
- Experts' consultation in varied areas of education.
- Better professional development of all grades involved in education.
- Communication between teachers both locally and overseas, to integrate different ideas and methodologies into their teaching.
- Collaboration between colleges.
- Technical expertise related to networks and automatic systems updates.
- Computer aided learning from anywhere and at any time convenient to the user.



## 2.3 Content evaluation



Information contained online, including blogs and social media, necessitates an informed level of digital literacy. It is common knowledge that the origin of this information cannot always be verified nor its veracity determined. To this extent, it is imperative that the curriculum is referred to in a holistic manner. Ideally, every bit of information which is classified as not suitable to students, should be restricted, however, this is a mammoth undertaking and for obvious reasons cannot be always guaranteed. In view of this, by educating students, empowerment will be given to them when these encounter information on the Internet which may be unsettling, threatening or offensive.

- Students will be taught to critically analyse data (both audio visual and in text form) before accepting it as de facto.
- They will be taught to use search effectively for their research over the Internet.
- An important part of the curriculum will as well be evaluating on-line material relevant to the different subjects they are being taught.
- Should students or teachers come across material which they recognise as unsuitable or inappropriate, they are to forward the URL to the Department of eLearning.
- Schools should emphasise that any material used from the Internet will not infringe copyright laws.
- Reliability regarding the source of the data being copied and the importance of intellectual property, will be also key features which will be taught to students whenever they include information from the Internet in their research.

## 3 Communication & Content

### 3.1 Site Content



The majority of schools already have excellent websites or blogs, on which the students can upload their projects and/or classwork. Nonetheless, on the Internet, one may encounter an abundance of websites and blogs where publications, projects or assignments can be uploaded. However, the MEDE stresses on the issue of security and therefore, encourages schools to upload students' work on the iLearn VLE. Any other blogs or websites which do not ask the user to login with a username and password cannot, be considered as positively secure. Sensitive data, in this regard, should never be deposited on any websites or blogs which do not require login. The iLearn VLE offers this level of security and peace of mind.

- Personal contact details should never be entered in any websites and blogs going to be used outside the iLearn VLE. It is advisable to enter generic details such as the name, address, email and telephone number of the school. No personal information pertaining to teachers or students should ever be divulged.

- Written consent should be sought from the individual or the parents, before any photos are uploaded on the school website. Photos should be screened beforehand and distinguishing features, such as faces should not be immediately recognisable.
- Names in full of students should be avoided and certainly not in caption or tagged to any photos.
- Any other item/s appearing in the uploaded photo/s should not lead to guessing one's identity in the same photo/s.
- Editorial privileges on websites outside the VLE should be, at the Head of School's disposal and he/she should make sure that any uploaded information is apt.
- Editorial rights within the VLE are the responsibility of the owner of the virtual room.
- The website in use should be accordance to publishing laws which safeguard intellectual property and authoring rights.

## 3.2 Virtual Platforms



Both the eLearning Virtual Environment and the schools information systems called e1, present a rich variety of benefits to educators and students, and also support the administration teams in schools.

- All users will be asked for a strong password to access content on the VLE. As with all other passwords, this should never be disclosed.
- MITA are contractually bound to keep track of all activity effected by users, especially communication.
- All users are informed of the acceptable use of iLearn. The terms are made available on the iLearn dashboard.
- Access to the VLE is granted upon registration. All members (especially within a school environment) will be granted clearance to various parts of the VLE as per access rights allotted to them.
- All users must respect rules governing intellectual property and should exercise due discretion when uploading content.
- At the termination of their last year in school, students should have their account deactivated or transferred on to their new school, provided that this would be a state school.

## 3.3 Use of email

Email has become so commonplace, yet, it is the staple means of communication for administrative and teaching grades and also students. Appropriate use of this powerful tool, certainly contributes to benefits in education and also makes possible, collaboration between schools, for instance, where projects are concerned. Again, as with all other instances of internet usage, the question of security must be dealt its due share.



Schools should determine the best use of email according to their needs, their students' and in line with the curriculum. Email addresses which contain users' names and surnames, such as emanuel.zammit@ilearn.edu.mt should not be assigned to students especially those of a young age, as this facilitates identification in an obvious way.

- Students should only send/receive emails to and from email addresses approved by the school and which contains the domain name @ilearn.edu.mt
- Students should report to their supervisor straight away, any offensive email in their inbox.
- All grades in a school should always use their MEDE-allotted email addresses when officially communicating with relevant Directorates.
- When sending emails, students should be made aware of what's acceptable and what's not. For instance, no attachments containing photos or videos are allowed in emails, without the express consent of whoever appears in the photo/video. Any emails sent, which might be of distress, annoyance or deemed as bullying to the recipient/s will constitute a serious breach of the policy and will absolutely under no circumstance, be tolerated.
- The use of netiquette in emails is fundamental and the content should always be vetted, especially if emails are sent to foreign parties and/or overseas. Emails originating from schools should be treated the same way as when paperwork containing the letterhead of the school is mailed.

### 3.4 Communication & social media



Filtering may be imposed on online chat, social media sites and other forms of online communication. Almost certainly, these forms of communication would be familiar and readily accessible, outside school hours.

All grades should be conscious of the risks of using social networking sites or publishing material on them, whether this is carried out in a professional way or on a personal basis. Before uploading on these sites, teaching grades must make sure they will not be compromising their profiles. At the same time, anything which is about to be put online, has to be carefully checked and re-considered before going ahead. Any inappropriate material which is uploaded by teachers might, negatively reflect on their professional status and might also be in breach of the teachers' code of ethics.

Students should also be taught against uploading any personal information without a second thought. Once available online, information can be disseminated very quickly and deleting or hiding it can be, oftentimes too late. Traces of online activity can prove hard to retract as well. As such, the best tool against committing this mistake is, to empower schools to teach students to communicate online safely and not to give away any personal information. With this in mind, the Department of eLearning is pushing forward a programme regarding digital citizenship. Users will be shown how to keep their personal information private, such as refraining from using actual names and surnames, addresses (of residence and email),

referring to the school they attend at, mentioning friends' names or those of next-of-kin, revealing any particular extra-curricular activities and where they are carried out.

Needless to say, besides the above, users should never tag themselves (or others) in online photos and/or identify themselves (or others) in videos posted online. And most importantly, they should never accept any on-line invitations to meet up in person...one might never know.

- Any teachers wishing to use online communications with their students should do so, within the curriculum framework and via the iLearn platform. When other online resources are going to be used besides iLearn, for communicating, teachers should take into consideration security first and foremost, as well as, whether the sites in question, are appropriate or not vis-à-vis the age of their students. This can be done, for instance, by reading the terms and conditions. Before proceeding, the school administration should be informed. A letter of consent could be then issued, only if, this social-media-related activity falls within the school policy.
- On the same note, personal blogs or wikis outside the approved VLE, should carry a letter of consent from the administration as applicable above. The blogs and wikis should be password-protected.
- Students will be taught the best practice when publishing online educational material. This will take place in accordance to their age bracket as well. Again, teachers are highly encouraged to use the resources in the VLE.
- Hand-in-hand with the issue of privacy and security, students will be taught to establish passwords to their accounts, to deny access to any unwarranted requests and to block any undesired communication. They will also be advised to add to their lists, only friends whom they know in person and to create private profiles to discourage unfamiliar requests or invitations. These points will also feature in the Digital Citizenship programme.
- Members of school staff should refrain from posting online their personal views or details about the school they work at. This is especially true should their posts be possibly interpreted as, being insulting, bullying or threatening in nature.
- Any school-related activities filmed or recorded by parents, should not be uploaded online without the parents being first aware, whether this is permissible or not according to school policy.
- From time-to-time, the school will update parents regarding the use of social networks, social media, blogs and wikis (within and outside the VLE), especially if, usage of the aforementioned media requires a minimum of age.
- Personal use of networking media, social media and publication (personal) on sites will be a matter of discussion with teaching grades. Same applies for online security and professional discretion when using the above media. Teaching grades will have to be conversant with what's being expected of them as stipulated in the school policy of responsible

use of the Internet.

- Teaching grades will be expected to hold back from engaging into any private online communication with their students or their students' parents or guardians.

### 3.5 Mobile devices (including BYOD)



The term “mobile devices” encompasses any portable device, with access to Internet or other forms of networking. These include tablets (with Apple, Android, Windows or any other operating system), e-readers, mobile phones or smartphones, iPod Touch and digital cameras.

Mobile devices create a diversity of channels of communication, hence, the need of setting up a policy which prohibits students, carrying them around, on the school premises. Some might disagree, arguing that this policy is not realistic. Students might still smuggle in class, mobile devices and the teacher would be none the wiser, if he/she were to be recorded during the delivery of the lesson. Therefore, to counter this from happening, an atmosphere of mutual respect between students and teachers has to be instilled. Teaching grades must also set the example by, using their mobile devices and/or those provided by the school, in a responsible way.

The use of mobile devices in school has to be dictated by the school policy and discretion. The following principles are the backbone of this policy:

- It is imperative that users are safe from bullying, threats and disturbing online content, within the school environment.
- Access to online digital resources is made available to all users, guaranteeing the best possible level of education.
- Users would be given guidelines as to what are their responsibilities and what professional conduct is expected of them, when communicating online.
- It is up to the teacher in class, to choose what mobile devices to allow, provided this serves an educational purpose.
- Schools can liberally determine what forms of devices are acceptable, within the school limits and turn down any which, they deem unsuitable or unnecessary.

The following tips can guide schools to draft an effective policy:

- Any mobile devices brought to school, are the users' sole responsibility. The school may not be held accountable if the device/s get damaged, lost or stolen.
- A team of teachers (not individuals) can be entrusted by the school management, to conduct searches in student/s bags and confiscate mobile devices. This would take place in instances where there is a strong suspicion that, the school policy regarding the use of mobile devices has been abused. Other justifiable instances would be defiance of

school discipline regulations or simply the fact that the mobile device in question, does not fall within the acceptable list of devices, which can be brought to school. In cases where there is enough suspicion that, the material recorded and stored on the mobile device may constitute a criminal act, the police are to be called to intervene and investigate.

- It is strictly forbidden to all users, to send any offensive messages or other inappropriate material to other members within the school environment.
- Mobile devices can be brought into a lesson and/or on the school premises, only against approval and/or if the device is to be part of a curriculum-related activity.
- Specific places on the school premises, such as toilets or changing rooms are strictly out-of-bounds to the use of mobile devices. This is also applicable to specific situations such as clashes between members of the school community.
- During breaks and lessons (even substitute lessons), the use of mobile devices is prohibited, unless, it is part of an approved activity. Unauthorised and unsupervised use of mobile devices is neither desirable nor allowable.
- If any teacher feels the need to contact the parents/guardians of a particular student, this should happen through the official channels in place at school, such as by iLearn email account or the school landline. In extraordinary circumstances, where the teacher has to make use of his/her mobile device, this should occur only after the school management team has been informed and has found no objection.
- Teachers may use only devices provided by the school to film school events or snap photos of students engaged in educational activities. In the event that, personal devices are involved at aforementioned events/activities, teachers should check and make sure that the use of their own personal devices does not go against the established school policy.
- The school must ensure that all necessary steps are taken, to uphold its set policy regarding the use of mobile devices.

### 3.6 Video Conferencing



Video conferencing (which includes Skype and the Meeting tools on the VLE) facilitates audio visual communication between parties, located at different geographical locations. One can imagine the potential, this mode of communication, opens for education. Video conferencing in schools is recommended, primarily supported over the school network.

- Before engaging students in any video conferencing activities, teachers should be familiar with the agreement between the school and parents, as set out in the policy.
- Any hardware used in video conferencing should be disconnected and stored in a safe location, after use. No hardware should be left

unattended, or in standby or auto mode.

- Students should seek their teacher's permission before accepting video conferencing requests.
- Video conferencing sessions should be supervised and should be adapted according to the students' age group and capabilities.

### 3.7 Cyberbullying



Bullying has taken on a new form with the advent of Internet. It can be defined as "harassment by using technology and/or online media to intimidate, afflict or taint and ruin one's dignity, by means of messages and emails, SMSs or photos sent via mobile phones, social media sites, blogs, chat rooms and discussion groups." (Addressing Bullying Behaviour in School Policy, 2014)<sup>4</sup>.

In the majority of cases, mobile devices and Internet use, is done appropriately and is a positive and creative experience. However, the possibility of abuse/misuse is a stark reality. Users should therefore, be taught and informed how cyberbullying differs from other forms of traditional bullying, how it can ruin lives and how to counteract its instances. A zero-tolerance policy to cyberbullying (and other forms of bullying, for that matter) has to be adopted in schools. More details can be found in the policy on how to tackle bullying behaviour, namely:

- Clear procedures to investigate alleged instances of bullying.
- Specific ways to offer support to victims of bullying behaviour.
- All instances of cyberbullying are to be logged and reported by schools.
- All necessary steps will be taken by the school, to identify the bullying person, whenever possible and feasible. This might include going through digital logs at school, identifying and interviewing witnesses and if needed, collaboration with the ISP and the police.
- The school, its staff, students and the parents must stand united to foil cyberbullying and its nefarious consequences.

### 3.8 Data protection



The sheer amount of digital information concerning students, families and employees is substantial and it gets more defined by time. This data, of course, is essential for improving client services, however if mis-handled it can get stolen and misused. The Data Protection Act of 2012, (DPA\_amended2012.pdf), states that the individual has every right to know what personal details are being used and to what end. The Data Protection Act ensures that a level of transparency is maintained whenever personal data is in one way or another, utilised.

Schools are also a hub of personal data and therefore, must be aware of their obligations as stipulated by the Data Protection Act. This section is in



essence, reiterating the fundamental point that all personal data must be protected. Data must be input, processed, output and transferred within the framework set by the Data Protection Act.

## 4 Implementation

### 4.1 Policy in practice Students



Many of the students, these days, will be conversant with Internet use. It is thus, crucial to involve them in discussions (suitable to their age) about best use of the Internet, as part of the Digital Citizenship programme, in schools. As is crucial as well, that the students get reminded of the school policy, regarding proper use of Internet:

- All Internet activity on the school network will be monitored.
- Acceptable behaviour whilst being online should be at the core of the curriculum. Safe and responsible use of the Internet should be emphasised amongst the students.
- Digital literacy will leave its mark on a wide variety of subjects. Part of its mark will be the safe use of online resources, both at school and from home.
- Posters promoting appropriate use of the Internet and/or leaflets advocating such should be, on display in each room, where Internet access is possible. The leaflets might also contain an abbreviated version of the school policy regarding acceptable use of the Internet.
- Internet safety and responsibility will be two key areas which will be boosted, across the framework of the curriculum.

### 4.2 Policy in practice Teachers



It is vitally important that all educators feel confident when integrating technology into their teaching. The effectiveness of the school policy regarding proper use of online material, can only be appreciated when educators abide by its rules and set patterns of behaviour. As expected, educators should be given the opportunity to discuss educational issues and develop newer, better strategies to amalgamate to their teaching. Particular attention has to be dedicated to the use of devices during school hours and especially, if the use of these devices is not done via the school network. Teaching grades are expected keep confidential information about the school to themselves since this forms part of their professional conduct as well. If doubts arise about the correct use of ICT, teachers should immediately refer their concerns to the Head of School.

- The school policy regarding acceptable online use and behaviour should be a consultative process, which involves teaching grades.
- Teaching grades must be made aware that their online activity at school is monitored. This will serve as a deterrent against unprofessional behaviour and promote proper demeanour during online use.



- Training targeting proper Internet use will be given to school personnel, both to enhance their professionalism and also to keep them updated on a personal level.

- Attention must be drawn to all grades that improper online activities outside school, may negatively impact their image and reputation as professionals. In such occurrences, legal and disciplinary actions may be triggered, if there is undeniable proof that the teaching profession has been tainted because of such irregularities. (refer to the Teachers' Code of Ethics and Practice, 2012)<sup>5</sup>

### 4.3 Policy in Practice Parents



Parents must be informed of and be vigilant against all perils of online communication, social media and mobile devices (such as tablets and smartphones), which might unwittingly put their children at risk. Thanks to the iLearn VLE, the Department of eLearning will keep parents informed as to the best practices their children can follow, when accessing the Internet.

- Parents will be notified of the Policy of Acceptable Online Behaviour and the Policy of Responsible Use of Online Resources in the Access to Parents room on the iLearn VLE.

- Collaboration with parents will be actively sought. The school and parents depend on each other for their students'/children's benefit. This can be achieved by demonstrations, practice sessions and suggestions as to what online resources are best suited to the children and how to maintain online security at home.

- Constant updates to parents will guarantee a stronger involvement with the school to keep students/children safe whilst being online, both during and after school hours.

- In case of improper online behaviour, the parents must be approached and informed, in a confidential and compassionate way. There is no need for sensationalism which might in turn, cause tension.

- Advice regarding filtering, educational and leisure activities (which might necessitate a responsible approach to Internet use, amongst others) will be made available on the iLearn VLE to the students' parents/guardians by visiting the Access to Parents room.

### 4.4 Handling complaints

Parents and teachers alike must be familiar of the standing procedure to follow, when reporting or submitting complaints regarding the online protection and security. Immediate action must be taken upon receipt of these reports or complaints regarding breaches of correct, Internet use policy. Of course, facts must be established first and foremost, such as whether the incident took place within the school or at home. Minor breaches of the aforementioned policy can be tackled by the teachers in line with the usual disciplinary methods, employed at school. More sensi-

tive cases may lead to sanctioning at various levels according to the severity of the case. Any information pertaining to the case must be archived, for instance, emails, SMSs and any other form of correspondence.

- Any incidents regarding inappropriate Internet use, should be addressed to the SMT.
- Any complaints involving improper use of the Internet by teachers should be, reported to the Head of School.
- Students and parents/guardians will be informed as to the procedure to follow, regarding any complaints.
- Students, parents/guardians and teachers may collaborate to find an amicable solution should any incidents of Internet misuse occur.
- In extreme circumstances where, the police have to be involved, acting sooner rather than later will lead to a swifter outcome. Verifying a legal standpoint and coming up with strategic solutions, will also avoid any setbacks to getting back to the schooling routine.

## Notes

<sup>1</sup> Young users will be made aware of the policy progressively according to their age.

<sup>2</sup> Grades means Kindergarten Assistants, Learning Support Assistants, teachers, senior management, college principals, education officers, pre-service teachers.

<sup>3</sup> Parents includes guardians.

<sup>4</sup> <https://education.gov.mt/en/Documents/Addressing%20Bullying%20Behaviour%20in%20Schools.pdf>

<sup>5</sup> <https://education.gov.mt/en/Ministry/Documents/New%20Code%20of%20Ethics%20Doc%20EN.pdf>